

EXHIBIT 3

Gregory Rattray
2/12/2025

<p>1 UNITED STATES DISTRICT COURT 2 SOUTHERN DISTRICT OF NEW YORK 3 4 SECURITIES AND EXCHANGE) 5 COMMISSION,) 6 Plaintiff,) 7) Civil Action No. 8 v.) 23-cv-9518-PAE 9) 10 SOLARWINDS CORP. and) 11 TIMOTHY G. BROWN,) 12) 13 Defendants.) 14) 15 VIDEO RECORDED EXAMINATION OF 16 GREGORY RATTRAY 17 WEDNESDAY, FEBRUARY 12, 2025 18 NEW YORK, NEW YORK 19 20 21 22 23 CERTIFIED STENOGRAPHER: 24 JESSIE WAACK, RDR, CRR, CRRR, NYRCR, NYACR, 25 CCR-NJ (No. 30XI008238700) CSR-TX (No. 11958) CCR-WA (No. 21007264), CSR-CA (No. 14420), REALTIME SYSTEMS ADMINISTRATOR JOB NO. 250212JWAA</p> <p style="text-align: center;">1</p>	<p>1 A P P E A R A N C E S 2 3 ON BEHALF OF THE PLAINTIFF: 4 SECURITIES AND EXCHANGE COMMISSION 5 BY: CHRISTOPHER CARNEY, ESQ. 6 BY: JOHN TODOR, ESQ. 7 BY: CHRISTOPHER BRUCKMANN, ESQ. 8 BY: KRISTEN WARDEN, ESQ. (Remote) 9 BY: LORY STONE, ESQ. (Remote) 10 100 F Street, N.E. 11 Washington, D.C. 20549 12 PHONE: 800-732-0330 13 EMAIL: Carneyc@sec.gov 14 15 ON BEHALF OF THE DEFENDANTS: 16 LATHAM & WATKINS LLP 17 BY: SERRIN TURNER, ESQ. 18 BY: MATTHEW VALENTI, ESQ. (Remote) 19 1271 Avenue of the Americas 20 New York, New York 10020 21 PHONE: 212-906-1330 22 EMAIL: Serrin.turner@lw.com 23 24 25</p> <p style="text-align: center;">3</p>
<p>1 2 3 VIDEO RECORDED EXAMINATION of 4 GREGORY RATTRAY, taken before 5 JESSICA R. WAACK, Registered Professional 6 Reporter, Registered Merit Reporter, 7 Certified Realtime Reporter, Registered 8 Diplomat Reporter, California Certified 9 Realtime Reporter, New Jersey Certified Court 10 Reporter (License No. 30XI008238700); Texas 11 Certified Shorthand Reporter (License No. 12 11958); Washington State Certified Court 13 Reporter (License No. 21007264); California 14 Certified Shorthand Reporter (License No. 15 14420); New York Association Certified 16 Reporter, New York Realtime Court Reporter 17 and Notary Public of Washington, D.C. and the 18 States of New York, Pennsylvania, Delaware, 19 Maryland and Virginia, at Latham & Watkins, 20 1271 Avenue of the Americas, New York, New 21 York, on Wednesday, February 12, 2025, 22 commencing at 9:41 a.m. and concluding at 23 6:46 p.m. 24 25</p> <p style="text-align: center;">2</p>	<p>1 A P P E A R A N C E S 2 3 ON BEHALF OF THE DEFENDANTS: 4 LATHAM & WATKINS LLP 5 BY: SEAN M. BERKOWITZ, ESQ. 6 BY: MAURICE BAYNARD, ESQ. 7 330 North Wabash Avenue, Suite 2800 8 Chicago, Illinois 60611 9 PHONE: 312-777-7016 10 EMAIL: Sean.berkowitz@lw.com 11 12 A L S O P R E S E N T 13 (REMOTE) 14 ANNIE GRAVELLE 15 BECKY MELTON 16 17 A L S O P R E S E N T 18 19 DANNY ORTEGA, videographer 20 ERIC COLE 21 ROZALIA (ROZI) KEPES 22 23 --oOo-- 24 25</p> <p style="text-align: center;">4</p>

Gregory Rattray
2/12/2025

1	INDEX TO EXAMINATION	
2	WITNESS: GREGORY RATTRAY	
3		
4	EXAMINATION	PAGE
5	BY MR. CARNEY	10
6	BY MR. TURNER	303
7	BY MR. CARNEY	309
8		
9	INDEXED PAGES	
10		PAGE
11	GREGORY RATTRAY, sworn	9
12	REPORTER CERTIFICATE	313
13	DECLARATION UNDER PENALTY OF PERJURY	314
14	ERRATA SHEET	315
15		
16		
17	INFORMATION REQUESTED	
18	None	
19		
20	WITNESS INSTRUCTED NOT TO ANSWER	
21	None	
22		
23		
24		
25		
	5	

1	INDEX TO EXHIBITS	
2	WITNESS: GREGORY RATTRAY	
3	Wednesday, February 12, 2025	
4	MARKED	DESCRIPTION PAGE
5	Exhibit 10 Ticket: 260058;	
6	SW-SEC-SONY_00050922	176
7	Exhibit 11 SolarWinds Development Process	
8	slide deck	199
9	Exhibit 12 Final Security Review SRM	
10	(2019.4); SW-SEC-SONY	
11	_00055119	205
12	Exhibit 13 Email chain ending on	
13	November 18, 2019;	
14	SW-SEC00254254	217
15	Exhibit 14 MSP Products Security	
16	Evaluation - confidential -	
17	July 2019; SW-SEC00166790	231
18	Exhibit 15 Final Security Review	
19	ipMonitor (Doberman - 2019.4);	
20	SW-SEC-SONY_00069825	237
21	Exhibit 16 Final Security Review IPAM	
22	(2019.2 Finn);	
23	SW-SEC-SONY_00055006	240
24		
25		
	7	

1	INDEX TO EXHIBITS	
2	WITNESS: GREGORY RATTRAY	
3	Wednesday, February 12, 2025	
4	MARKED	DESCRIPTION PAGE
5	Exhibit 1 Gregory Rattray expert report	
6	dated November 22, 2024	41
7	Exhibit 2 Expert report of Gregory	
8	Rattray dated November 22,	
9	2024	42
10	Exhibit 3 Article, "JPMorgan Reassigns	
11	Security Team Leader a Year	
12	After Data Breach"	91
13	Exhibit 4 Article, "Building a Focused	
14	Approach to Cyber Defense"	99
15	Exhibit 5 "SolarWinds Security	
16	Statement"	119
17	Exhibit 6 SARF dated December 12, 2017;	
18	SW-SEC-SONY_0005545	131
19	Exhibit 7 Ticket : 193821;	
20	SW-SEC-SONY_00049602	147
21	Exhibit 8 Ticket : 202365;	
22	SW-SEC-SONY_00047323	159
23	Exhibit 9 MailAssure User Access	
24	Follow-Ups	171
25		
	6	

1	INDEX TO EXHIBITS	
2	WITNESS: GREGORY RATTRAY	
3	Wednesday, February 12, 2025	
4	MARKED	DESCRIPTION PAGE
5	Exhibit 17 Native document;	
6	SW-SEC00168780	285
7		
8	** EXHIBITS BOUND SEPARATELY ***	
9		
10		
11	--o0o--	
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
	8	

Gregory Rattray
2/12/2025

<p>1 *****</p> <p>2 PROCEEDINGS</p> <p>3 February 12, 2025, 9:41 a.m.</p> <p>4 New York, New York</p> <p>5 *****</p> <p>6 THE VIDEOGRAPHER: We are now on the</p> <p>7 record.</p> <p>8 My name's Danny Ortega, and I'm the</p> <p>9 legal videographer for Gradillas Reporting.</p> <p>10 Today's date is February 12, 2025, and the time is</p> <p>11 9:41 a.m.</p> <p>12 This video deposition is being held at</p> <p>13 1271 Avenue of the Americas, New York, New York,</p> <p>14 in the matter of SEC vs. SolarWinds Corp., et al.</p> <p>15 The deponent today is Gregory Rattray.</p> <p>16 All counsel will be noted on the stenographic</p> <p>17 record.</p> <p>18 The court reporter today is Jessie</p> <p>19 Waack, and will now swear in the witness.</p> <p>20 *****</p> <p>21 GREGORY RATTRAY, sworn</p> <p>22 on oath and/or affirmed, called as a witness</p> <p>23 herein, was examined and testified as follows:</p> <p>24 *****</p> <p>25 ///</p> <p style="text-align: center;">9</p>	<p>1 answer the question, and then we can take the</p> <p>2 break.</p> <p>3 And obviously the most important thing</p> <p>4 is that you're under oath the same as if you were</p> <p>5 in a court. So just give the answers truthfully</p> <p>6 to the best of your abilities.</p> <p>7 Is that okay?</p> <p>8 A. Yep, I understand.</p> <p>9 Q. Okay. And is there anything that</p> <p>10 would prevent you from being able to testify fully</p> <p>11 and truthfully today?</p> <p>12 A. No.</p> <p>13 Q. All right. And were you retained to</p> <p>14 provide expert services in this case?</p> <p>15 A. Yes, I was.</p> <p>16 Q. And who are you retained by?</p> <p>17 A. The -- Latham, the law firm.</p> <p>18 Q. Okay. And so you were hired directly</p> <p>19 by Latham & Watkins?</p> <p>20 A. Actually, Serrin, you know, I --</p> <p>21 THE WITNESS: I believe we were hired</p> <p>22 by Latham, right?</p> <p>23 You know, I don't know if the</p> <p>24 contractual relationship is with SolarWinds</p> <p>25 directly.</p> <p style="text-align: center;">11</p>
<p>1 EXAMINATION</p> <p>2 BY MR. CARNEY:</p> <p>3 Q. Good morning, Dr. Rattray.</p> <p>4 A. Good morning.</p> <p>5 Q. Just we haven't met before. My name's</p> <p>6 Chris Carney. I'm an attorney with the SEC.</p> <p>7 Sir, you've had your deposition taken</p> <p>8 before, right?</p> <p>9 A. Yes, I have.</p> <p>10 Q. So I know you know the ground rules,</p> <p>11 but let me just walk through some of them really</p> <p>12 quickly.</p> <p>13 So obviously our court reporter here</p> <p>14 is taking down everything we're saying, so it's</p> <p>15 important that we don't talk over each other. So</p> <p>16 even if you see where I'm going, just let me</p> <p>17 finish my question, and then you respond, and</p> <p>18 we'll have a clean record.</p> <p>19 Is that okay?</p> <p>20 A. Understood.</p> <p>21 Q. And we'll take breaks from time to</p> <p>22 time, but if at any point you need a break, just</p> <p>23 let me know.</p> <p>24 And the only thing I would ask is that</p> <p>25 if there's a question pending, that you just</p> <p style="text-align: center;">10</p>	<p>1 BY MR. CARNEY:</p> <p>2 Q. Okay. All right. When you get paid,</p> <p>3 is it Latham & Watkins that pays you?</p> <p>4 A. Again, my team invoices, and I get</p> <p>5 paid. So I'm actually not exactly sure --</p> <p>6 MR. TURNER: I can represent that</p> <p>7 SolarWinds pays the invoices.</p> <p>8 THE WITNESS: SolarWinds.</p> <p>9 BY MR. CARNEY:</p> <p>10 Q. And do you know how much you've been</p> <p>11 paid so far in this case?</p> <p>12 A. I don't know the total amount.</p> <p>13 Q. Okay. Do you know how many hours you</p> <p>14 personally have spent on this case?</p> <p>15 A. I would say 200-ish, yeah.</p> <p>16 Q. All right. And for purposes of this</p> <p>17 case, what do you consider your area of expertise</p> <p>18 to be?</p> <p>19 A. My area of expertise relevant to this</p> <p>20 case is, you know, understanding how companies,</p> <p>21 enterprises control their information environment,</p> <p>22 implement security controls.</p> <p>23 Q. Okay. And is there a field of</p> <p>24 expertise that you would fold that into?</p> <p>25 A. You know, different labels are used,</p> <p style="text-align: center;">12</p>

Gregory Rattray
2/12/2025

<p>1 but information security or cybersecurity.</p> <p>2 Q. Okay. And do you consider yourself an</p> <p>3 expert in cybersecurity?</p> <p>4 A. Yes, I do.</p> <p>5 Q. Okay. You don't hold a degree in</p> <p>6 computer science, do you?</p> <p>7 A. I hold a bachelor of science, but I</p> <p>8 don't hold a computer science degree.</p> <p>9 Q. And a bachelor of science in political</p> <p>10 science and military history, right?</p> <p>11 A. Yes, I do.</p> <p>12 Q. And have you taken any courses in</p> <p>13 computer engineering?</p> <p>14 A. I've taken courses in technology</p> <p>15 policy. I haven't taken any -- any university</p> <p>16 courses in computer science or engineering.</p> <p>17 Q. And your master's degree, as I</p> <p>18 understand, is in public policy; is that right?</p> <p>19 A. That's correct.</p> <p>20 Q. And you have a PhD in international</p> <p>21 security; is that correct?</p> <p>22 A. That's where I wrote -- at Tufts</p> <p>23 University where I wrote my dissertation on the</p> <p>24 future of cyber warfare.</p> <p>25 Q. And that was at the Fletcher School?</p> <p style="text-align: center;">13</p>	<p>1 at the time.</p> <p>2 Q. Can you remind me what year you</p> <p>3 received your PhD?</p> <p>4 A. 1998.</p> <p>5 Q. Did your PhD program require any</p> <p>6 courses in software security to complete the</p> <p>7 degree?</p> <p>8 A. No.</p> <p>9 Q. Did your PhD program require any</p> <p>10 courses in computer network security to complete</p> <p>11 the degree?</p> <p>12 A. No, it did not.</p> <p>13 Q. Have you ever taken a course in</p> <p>14 software security?</p> <p>15 A. I have not taken a course in software</p> <p>16 security.</p> <p>17 Q. Okay. Have you ever taken a course in</p> <p>18 computer network security?</p> <p>19 A. Again, I've done a lot of guided</p> <p>20 research by professors in the technology field</p> <p>21 that included, you know, information technology,</p> <p>22 computer technology, security controls, but it</p> <p>23 wasn't a formal course. It was a formal course in</p> <p>24 the sense that I got credit.</p> <p>25 It wasn't a, you know, predesigned</p> <p style="text-align: center;">15</p>
<p>1 A. That's correct.</p> <p>2 Q. And as I understand it, at the</p> <p>3 Fletcher School a PhD in international security is</p> <p>4 a concentration within the international relations</p> <p>5 PhD program; is that right?</p> <p>6 A. The Fletcher School is the Fletcher</p> <p>7 School of Law and Diplomacy. There's actually</p> <p>8 not -- you know, there's not a specific</p> <p>9 concentration inside the school for the PhD</p> <p>10 program. You know, you have to have areas of</p> <p>11 study. One of mine was technology policy.</p> <p>12 Q. Okay. And did your PhD course or</p> <p>13 program at Fletcher require any computer science</p> <p>14 courses?</p> <p>15 A. No computer science courses.</p> <p>16 Q. Did your PhD program require any</p> <p>17 courses in information security to complete the</p> <p>18 degree?</p> <p>19 A. I did research courses, sort of guided</p> <p>20 research courses with professors around the</p> <p>21 evolution of at that time a fairly nascent</p> <p>22 computer and information security, but there was</p> <p>23 no -- there was no formal course in information</p> <p>24 security.</p> <p>25 I'm not sure that such courses existed</p> <p style="text-align: center;">14</p>	<p>1 course. It was an independent-guided research</p> <p>2 course.</p> <p>3 Q. Okay. Did your PhD program require</p> <p>4 any courses in applied cryptography?</p> <p>5 A. No.</p> <p>6 Q. Okay. And have you taken any courses</p> <p>7 in applied cryptography?</p> <p>8 A. No.</p> <p>9 Q. All right. Have you personally</p> <p>10 designed any cybersecurity systems?</p> <p>11 MR. TURNER: Object to the form of the</p> <p>12 question.</p> <p>13 THE WITNESS: I designed quite a few</p> <p>14 cybersecurity systems in terms of programs that</p> <p>15 companies run. You know, red team operations and</p> <p>16 processes, vulnerability assessment, you know,</p> <p>17 processes, you know.</p> <p>18 So everything from major</p> <p>19 organizations, information security, you know,</p> <p>20 approaches to certain types of operations that</p> <p>21 take place inside those programs, I've designed</p> <p>22 those processes and programs.</p> <p>23 BY MR. CARNEY:</p> <p>24 Q. And you mentioned you did this for</p> <p>25 companies.</p> <p style="text-align: center;">16</p>

Gregory Rattray
2/12/2025

<p>1 Which companies did you design these 2 cybersecurity systems for?</p> <p>3 A. I designed the cybersecurity program 4 for JPMorganChase while I was the CISO. I helped 5 with the formulation of the nation cybersecurity 6 strategy when I was at the White House and then, 7 you know, at while -- in two different commands in 8 cybersecurity in the Air Force.</p> <p>9 Designed different programs including, 10 you know, the Air Force's red team and penetration 11 testing program.</p> <p>12 As a consultant, I've helped 13 companies design their programs both overall 14 cybersecurity programs and specific threat 15 intelligence and red team and penetration testing 16 programs.</p> <p>17 Q. Okay. And when you were -- let's use 18 JPMorgan for an example. That was the first one 19 you mentioned.</p> <p>20 When you designed their cybersecurity 21 program, were you responsible for any of the 22 technical implementation of that program?</p> <p>23 MR. TURNER: Object to form.</p> <p>24 THE WITNESS: I was, as the CISO, 25 responsible for the oversight of the entire</p> <p style="text-align: center;">17</p>	<p>1 monitoring, you're often using tools that are in 2 place on devices and networks to, you know, 3 monitor whether -- you know, whether these things 4 occurred.</p> <p>5 Q. And do you -- how are those tools 6 created?</p> <p>7 MR. TURNER: Object to form.</p> <p>8 THE WITNESS: You know, the tools are 9 created initially through coding, though the point 10 at which enterprises use them, they're usually 11 not -- there's no coding involved with the tools 12 at the point at which an enterprise deploys the 13 tools.</p> <p>14 BY MR. CARNEY:</p> <p>15 Q. Okay. And do you have the technical 16 skills and capability to deploy those tools 17 yourself?</p> <p>18 MR. TURNER: Object to form.</p> <p>19 THE WITNESS: There's a wide variety 20 of tools. Some of them are pretty simple. I'm 21 not a hands-on technologist.</p> <p>22 So, you know, the ones that are 23 relatively straightforward for a user to deploy, I 24 can deploy. 25 ///</p> <p style="text-align: center;">19</p>
<p>1 program including its technical implementation. 2 BY MR. CARNEY:</p> <p>3 Q. Did you do any of the actual coding 4 involved in creating the cybersecurity controls?</p> <p>5 A. You know, I did not do any coding. 6 The control structures included both technical 7 and, you know, nontechnical controls. You know, 8 the program as a whole, you know -- yeah, I 9 work -- design -- was responsible for the design 10 and oversight of the entire program.</p> <p>11 Q. Okay. With respect to you mentioned 12 technical controls, do you have the capability 13 yourself to code technical controls?</p> <p>14 MR. TURNER: Object to form.</p> <p>15 THE WITNESS: Technical controls often 16 don't involve coding, so I'm not a coder.</p> <p>17 BY MR. CARNEY:</p> <p>18 Q. Okay. What do they involve then if 19 they don't involve coding?</p> <p>20 A. You know, many involve -- if we're 21 talking about -- are we talking about technical 22 controls?</p> <p>23 Q. Yes, technical controls. Thank you, 24 sir.</p> <p>25 A. In a technical control such as network</p> <p style="text-align: center;">18</p>	<p>1 BY MR. CARNEY:</p> <p>2 Q. What about the tools that are deployed 3 at an enterprise level? Do you have the skill set 4 to be able to do that?</p> <p>5 MR. TURNER: Object to form.</p> <p>6 THE WITNESS: I think we'd have to get 7 a little more specific as to -- you know, again, 8 relatively simple, you know, user level tools are 9 deployed in an enterprise, and then there's more 10 sophisticated -- you know, there's more 11 complicated tools deployed.</p> <p>12 BY MR. CARNEY:</p> <p>13 Q. Well, I think you -- the example you 14 gave was network monitoring tools.</p> <p>15 Do you -- would you have the technical 16 capability to deploy network monitoring tools at 17 an enterprise level for, say, JPMorgan?</p> <p>18 A. No, I would not.</p> <p>19 Q. Okay. And what kind of skills would 20 someone need to have to do that?</p> <p>21 A. So we're talking about the skills 22 necessary to deploy a network monitoring system?</p> <p>23 Q. Yes, Doctor.</p> <p>24 A. And just deploy it, right? Are we 25 talking separate from the operation of that --</p> <p style="text-align: center;">20</p>

Gregory Rattray
2/12/2025

<p>1 Q. Just to deploy it.</p> <p>2 A. Yeah. You know, it would basically</p> <p>3 be, you know, experience in software deployment,</p> <p>4 which is usually residual in the -- you know, the</p> <p>5 architecture or infrastructure teams in a large</p> <p>6 enterprise.</p> <p>7 Q. Okay. Do you hold any cybersecurity</p> <p>8 certifications?</p> <p>9 A. Defining "certification" as -- can we</p> <p>10 just get a definition of what we mean by</p> <p>11 "certification"?</p> <p>12 Q. Well, I'll give you an example.</p> <p>13 Are you familiar with CompTIA, and</p> <p>14 that's C-o-m-p-T-I-A?</p> <p>15 A. Yes, I am.</p> <p>16 Q. And they offer cybersecurity</p> <p>17 certifications, right?</p> <p>18 A. Yes, they do.</p> <p>19 Q. And do you hold any of those?</p> <p>20 A. I do not.</p> <p>21 Q. Are you familiar with -- and this is</p> <p>22 all caps I-S-C 2, which is the International</p> <p>23 Information Systems Security Certification</p> <p>24 Consortium?</p> <p>25 A. Yes, I am.</p> <p style="text-align: center;">21</p>	<p>1 security statement for this litigation, had you</p> <p>2 ever read other company's security statements?</p> <p>3 A. Yes, I have.</p> <p>4 Q. And in what context? Why had you done</p> <p>5 that?</p> <p>6 A. Both in the context of, you know, I</p> <p>7 guess, you know, I want to make sure that we're</p> <p>8 talking -- when you say "a security statement,"</p> <p>9 you know, we might want to define that a little</p> <p>10 bit.</p> <p>11 If it's about public declarations of</p> <p>12 the company's security posture, you know, I just</p> <p>13 want to make sure that's the frame we're putting</p> <p>14 on it as the answer to the question.</p> <p>15 Q. Sure, sure.</p> <p>16 So I'm talking now about the</p> <p>17 SolarWinds's public-facing --</p> <p>18 A. Yep.</p> <p>19 Q. -- security statement that's at issue</p> <p>20 in this case --</p> <p>21 A. Yes.</p> <p>22 Q. -- as well. I'm asking about</p> <p>23 analogous security statements at other companies.</p> <p>24 A. Yes, I've seen them. You know, at</p> <p>25 JPMorgan, when I was a CISO there, we made --</p> <p style="text-align: center;">23</p>
<p>1 Q. And what is ISC2?</p> <p>2 A. It's a number -- one of a number of</p> <p>3 different bodies in the -- in the cybersecurity</p> <p>4 field that, you know, works to train and certify</p> <p>5 people.</p> <p>6 Q. Okay. And ISC2 offers cybersecurity</p> <p>7 certifications, right?</p> <p>8 A. I believe they do.</p> <p>9 Q. And do you hold any of those?</p> <p>10 A. I do not.</p> <p>11 Q. And do you have -- I'll spell it out</p> <p>12 -- C-I-S-S-P certification?</p> <p>13 A. I do not.</p> <p>14 Q. Do you have any -- do you have any</p> <p>15 SANS GSEC certification?</p> <p>16 A. I'm not sure what those certifications</p> <p>17 are. I don't hold them.</p> <p>18 Q. And are you familiar with CertNexus,</p> <p>19 and that's C-e-r-t and then capital N-e-x-u-s?</p> <p>20 A. I don't believe I am.</p> <p>21 Q. And, Doctor, you're aware that this</p> <p>22 litigation involves SolarWinds's security</p> <p>23 statement, right?</p> <p>24 A. Yes, I am.</p> <p>25 Q. And before reading SolarWinds's</p> <p style="text-align: center;">22</p>	<p>1 that's why I wanted to clarify.</p> <p>2 We made public statements about our</p> <p>3 security that I don't think we put it in the form</p> <p>4 of a security statement like we see at SolarWinds.</p> <p>5 I've also seen them in consulting, you</p> <p>6 know, engagements that I've had, you know, much</p> <p>7 more similar to the SolarWinds situation.</p> <p>8 Q. Okay. And let me break that down.</p> <p>9 So have you ever written the</p> <p>10 public-facing securities statement of an</p> <p>11 organization?</p> <p>12 A. I have been involved in the -- you</p> <p>13 know, the creation, the establishment of, again,</p> <p>14 public-facing security statements.</p> <p>15 Again, I guess the question is, how</p> <p>16 close to the -- you know, how much am I looking at</p> <p>17 exactly the type of statement that SolarWinds had.</p> <p>18 But I've been -- I've certainly been</p> <p>19 involved in the creation of public-facing</p> <p>20 statements about security. You know, I think</p> <p>21 that's -- we can refine if necessary.</p> <p>22 Q. Sure. And about how many companies</p> <p>23 have you done that for?</p> <p>24 A. Again -- well, it probably gets to the</p> <p>25 idea that the way securities statements are, you</p> <p style="text-align: center;">24</p>

1 know, established publicly usually is not an
2 individual, you know, activity, and it wasn't in
3 the case of SolarWinds, right?

4 I've been involved in processes where
5 companies are deliberating about what to say about
6 their security posture, commenting on draft
7 language, drafting language at times.

8 **Q.** Okay. And are there specific
9 companies you can recall doing that for?

10 **A.** You know, again, certainly with
11 JPMorgan when we were making public statements
12 about security, I was involved in those.

13 And in consulting work, I, you know,
14 basically am under nondisclosure agreements about
15 the specifics of activities I undertook.

16 When I was the chief security advisor
17 to ICANN Internet Corporation For Assigned Names
18 and Numbers, we made -- you know, we made -- we
19 may have made statements. I don't remember
20 exactly, so I probably was involved during the
21 period I was there.

22 **Q.** Okay. And have you ever in your work
23 had to advise -- forgive me if this covers what
24 you already said.

25 But have you ever been called upon to

25

1 description of practices, I've done that over and
2 over again, yes.

3 **Q.** And have you ever had to advise a
4 company to modify its security statement, because
5 their practices didn't match what the security
6 statement said?

7 **A.** You know, I'm just -- I'm seeking to
8 recall. I think -- you know, I can't recall a
9 specific instance of modifying language related to
10 a public-facing statement.

11 Again, are we -- are we good with you
12 saying security statement, and me thinking about
13 this more broadly as, you know, public statements
14 made by companies related to their security? Are
15 we saying the same thing?

16 **Q.** Yeah, I think we're saying the same
17 thing.

18 **A.** Okay.

19 **Q.** All right. Let me delve in a little
20 bit in your expertise in cybersecurity.

21 And if it helps -- I'm going to hand
22 it to you in a little bit. I have your CV here.
23 So if you need it, let me know.

24 But where in your background do you
25 have expertise in access control?

27

1 advise a company on their security statement that
2 they were writing?

3 **A.** Again, you know, a lot of times
4 they're not called security statements, you know,
5 sort of -- but I have advised on the establishment
6 of public-facing security language for companies.

7 **Q.** Have you ever, in your work prior to
8 this case, had to analyze the security statement
9 of an organization to see if it matched what they
10 were actually doing?

11 **A.** I've conducted numerous assessments of
12 companies, cybersecurity postures, control
13 structures. That has informed in the cases where
14 I've been consulting my opinion about, you know,
15 things that they're going to say publicly. You
16 know, I would say that would be the way to
17 characterize my experience.

18 **Q.** Okay. Have you ever taken a
19 public-facing security statement and analyzed
20 whether what the company was doing matched what
21 they said in that public-facing security
22 statement?

23 **A.** You know, to the extent that which
24 security statements, you know, describe control
25 structures and you assess, you know, you know,

26

1 **A.** You know, starting in my military
2 career, you know, as we started to define, you
3 know, what we initially called information warfare
4 and then called cybersecurity cyber warfare, you
5 know, I was involved, you know, in the development
6 of approaches both -- you know, both policy and
7 procedural.

8 But also operational related to, you
9 know, how Air Force organizations, you know, would
10 need to implement that.

11 And then as commander of two separate
12 Air Force organizations, which in these cases were
13 cybersecurity organizations, we -- we were
14 required to implement the information security
15 practices of the Air Force as commander and,
16 therefore, had oversight of an information
17 security program which had detailed access control
18 provisions.

19 One of those organizations also wrote
20 the first set of what we call tactics, techniques
21 and procedures for cybersecurity, which would
22 have -- you know, which did include, you know, the
23 full set of things that an organization should
24 perform while the -- defending their networks,
25 which would include access controls. So that

28

<p>1 probably describes my Air Force experience.</p> <p>2 As, you know -- as a consultant, you</p> <p>3 know, in conduct of -- you know, information</p> <p>4 security assessments of organizations, I have led</p> <p>5 and reviewed assessment reports about the presence</p> <p>6 of access controls in a large number of</p> <p>7 organizations.</p> <p>8 In the JPMorgan role, we had -- access</p> <p>9 controls were, you know, part of the broader</p> <p>10 information security program where we had policies</p> <p>11 and procedures.</p> <p>12 I reviewed those policies and</p> <p>13 procedures as well as, you know, had metrics</p> <p>14 provided to me about the implementation of our</p> <p>15 policies and procedures. I think that's a fairly</p> <p>16 comprehensive review.</p> <p>17 MR. TURNER: I just want to flag for</p> <p>18 the court reporter, it's "tactics, techniques and</p> <p>19 procedures."</p> <p>20 BY MR. CARNEY:</p> <p>21 Q. All right. So thank you for that.</p> <p>22 In addition reviewing the policies and</p> <p>23 procedures and receiving metrics on the</p> <p>24 implementation of those policies and procedures,</p> <p>25 do you have any sort of technical skills or acumen</p> <p style="text-align: center;">29</p>	<p>1 You know, similar to password, you</p> <p>2 know -- the implementation of password controls,</p> <p>3 user identification is usually an element in most,</p> <p>4 you know -- some policy and procedure approaches</p> <p>5 around naming conventions for users on a network.</p> <p>6 So I've certainly been involved in the</p> <p>7 development of, you know, user access controls and</p> <p>8 agreements, which, you know, specify the level of,</p> <p>9 you know -- like, how people will be identified in</p> <p>10 a user identification system.</p> <p>11 I'd say that probably characterizes my</p> <p>12 experience.</p> <p>13 Q. And similar to my earlier question, do</p> <p>14 you have any sort of technical skills as it</p> <p>15 relates to implementing user identification</p> <p>16 requirements?</p> <p>17 MR. TURNER: Object, again, to form.</p> <p>18 "Technical."</p> <p>19 THE WITNESS: Right. The</p> <p>20 implementation of user identification systems is</p> <p>21 not a particularly technical activity, you know,</p> <p>22 in terms of it's mostly a process, you know,</p> <p>23 setting activity.</p> <p>24 And, again, I've described and I can</p> <p>25 repeat if you like, sort of my, you know, my</p> <p style="text-align: center;">31</p>
<p>1 as it relates to designing access controls?</p> <p>2 MR. TURNER: Object to form.</p> <p>3 THE WITNESS: You know, I've been</p> <p>4 involved in, you know, deciding, you know, how</p> <p>5 strong certain access controls, things like, you</p> <p>6 know, password complexity and how hard should we</p> <p>7 make it or provisions for -- in a data loss</p> <p>8 prevention systems, you know, what are the things</p> <p>9 that would be flagged down to the implementation</p> <p>10 level of those systems in terms of what would be</p> <p>11 present in the implementations of those systems.</p> <p>12 Again, I'm not a coder, so I did not</p> <p>13 go down to the coding level in my experience with</p> <p>14 the implementation of security controls.</p> <p>15 BY MR. CARNEY:</p> <p>16 Q. Okay. What is -- what about the sort</p> <p>17 of same question as it relates to user</p> <p>18 identification?</p> <p>19 What's your experience as it relates</p> <p>20 to user identification?</p> <p>21 A. You know, both as a user in many</p> <p>22 organizations -- we can go through them, but I</p> <p>23 don't think we need to, you know, in the different</p> <p>24 sort of organizations I've been involved with over</p> <p>25 the years.</p> <p style="text-align: center;">30</p>	<p>1 experience in the process setting side of things.</p> <p>2 You know, the tools are, you know,</p> <p>3 developed and deployed as we've already discussed.</p> <p>4 But, you know, at an enterprise level,</p> <p>5 it's almost all a decision about the processes you</p> <p>6 develop and deploy on those tools in order to</p> <p>7 achieve a security control, which, again, I've</p> <p>8 been involved pretty directly in that.</p> <p>9 BY MR. CARNEY:</p> <p>10 Q. Okay. Have you -- do you have any</p> <p>11 involvement or experience in developing software?</p> <p>12 MR. TURNER: Object to form.</p> <p>13 THE WITNESS: I have certainly, you</p> <p>14 know, overseen programs that are, you know,</p> <p>15 responsible for ensuring the security and the</p> <p>16 development of software.</p> <p>17 I'm not a coder, so, you know, if the</p> <p>18 question is, do I do coding, I don't do coding.</p> <p>19 BY MR. CARNEY:</p> <p>20 Q. And so what was your responsibility</p> <p>21 for ensuring the security in the development of</p> <p>22 software?</p> <p>23 A. Oversight of and then consulting on</p> <p>24 secure software development, you know, procedures</p> <p>25 in -- you know, in the development environment in</p> <p style="text-align: center;">32</p>

Gregory Rattray
2/12/2025

<p>1 different countries -- not countries -- companies. 2 Q. And what different companies were you 3 involved in the secure development lifecycle 4 process? 5 A. At JPMorgan, we had a secure 6 development, you know, emphasis -- right? -- you 7 know, inside the security programming in 8 conjunction with the application developers in the 9 company. 10 I -- you know, in consulting reviews, 11 you know, again, secure development is an element 12 of most security reviews at this stage, so I've 13 been involved in sort of numerous reviews and 14 assessments of secure development environments. 15 Q. And what -- what kind of software was 16 JPMorgan developing that used the -- can I call it 17 SDL process? 18 A. Yeah, call it -- yeah, we'll use SDL. 19 You know, JPMorgan develops a wide 20 variety of applications for both, you know, 21 internal use and external, you know, use by 22 customers. You know, very large numbers of 23 different applications was -- this process was -- 24 was part of. 25 Q. And when you were the CISO at</p> <p style="text-align: center;">33</p>	<p>1 the company -- you know, attune to that? 2 Are we feeding our knowledge of how 3 threat actors behave into, you know, processes 4 like software development. So I have a lot of 5 experience with, you know, threat modeling. 6 Q. So as an expert in cybersecurity, how 7 would you define threat modeling? 8 A. You know, in practice, and, again, 9 across a wide variety of organizations and 10 experiences, threat modeling is, you know, used 11 fairly broadly to describe, you know, how a -- a 12 sort of process or a callout to, you know, look at 13 risks that, in particularly security risks or 14 cybersecurity threats and, you know, understand 15 how that is affecting, you know, the security 16 process you're either implementing or the project 17 that you've got underway. 18 That's how I think about threat 19 modeling. 20 Q. And I know from your report, you're 21 familiar with NIST, right? 22 A. The National Institute of Standards 23 and Technology? 24 Q. Yes. 25 A. Yes, I am.</p> <p style="text-align: center;">35</p>
<p>1 JPMorgan, you had some involvement in that 2 process? 3 A. I had oversight of the, you know -- 4 in, you know, review of the processes we had asked 5 the technology teams to implement. 6 Q. The SDL process that JPMorgan 7 followed, was that -- you know, was that based on 8 the Microsoft SDL process? 9 A. I'm not at liberty to get into sort of 10 any specifics because of my exit agreement with 11 JPMorgan about specifics inside the JPMorgan 12 security program. 13 Q. Okay. Have you ever personally 14 conducted threat modeling? 15 A. Many times. In basically the idea 16 that a security program, a -- you know, the 17 development of technology for a company needs to 18 take into account, you know, threat-based risks, 19 you know. 20 You know, I've been the -- many person 21 identifying threats to organizations, you know, at 22 the organizational, even the national level in 23 terms of, you know, how -- who are threat actors? 24 How do they behave? How do they pose 25 risk to companies? Are the control structures in</p> <p style="text-align: center;">34</p>	<p>1 Q. And you're familiar with ISO? 2 A. The institute, the International 3 Standards Organization. Yeah, I'm aware of both 4 of those organizations. 5 Q. And are you familiar with those 6 organizations' specific threat model structures 7 that they have put out? 8 A. I've not yet -- I don't know that 9 either organization's put out any threat modeling. 10 They may have, right? I'm more familiar with 11 cybersecurity frameworks that they've, you know, 12 put out. 13 Q. And I guess what I'm trying to 14 understand is that the way you describe threat 15 modeling, you don't think of it necessarily as a 16 specific set of defined activities; is that fair 17 to say? 18 A. That's fair. I mean, there's -- a lot 19 of people do it a lot of different ways, in my 20 experience. 21 Q. And if a company was performing threat 22 modeling, what sort of evidence would you expect 23 to see? 24 A. I mean, you know, one would want to 25 see, you know, evidence that they were considering</p> <p style="text-align: center;">36</p>

Gregory Rattray
2/12/2025

<p>1 threats that security concerns were baked into, 2 you know, development processes for technology 3 that were, you know, being considered that, 4 again -- you know, the notion that threat-based 5 risks were being considered as, you know -- you 6 know, and then incorporated in the activities that 7 were being -- you know, were underway. 8 That's how I think about, you know, 9 both threat modeling and, you know, what you would 10 be looking for in order to evidence the presence 11 of it. 12 Q. And you've touched on a bit your 13 experience with cybersecurity assessments. 14 Have you ever had an experience in 15 which an organization was not following some of 16 the cybersecurity policies that it professed to 17 follow? 18 A. You know, in general -- in general, 19 when one does an assessment, it's not a binary 20 sort of determination of, you know, follow versus 21 not follow. 22 It's, you know -- you know, an 23 assessment of the full set of procedures, 24 understanding evidence that you have available to 25 you.</p> <p style="text-align: center;">37</p>	<p>1 organization that said it had a policy is just 2 fundamentally absent in the performance of that. 3 Because, again, it's a -- sort of a 4 gradation from, you know, the presence of the 5 call-out to do something to how much is it being 6 done, right? You know, either more or less. 7 Q. Okay. And I just want to back up a 8 second to -- before we get too far away from it. 9 You had talked about -- when I asked 10 you whether you personally conducted threat 11 modeling, and you said that you had done it many 12 times basically in the idea that in a security 13 program, you need to take into account 14 threat-based risks and identify threats to 15 organizations and threat actors. 16 And I'm just wondering, the sort of 17 steps that you listed that you've personally done, 18 would you consider these to be standard steps of 19 threat modeling in the cybersecurity field? 20 A. You know, I don't think there's a 21 standard in this area. This area in particular is 22 one of those where the concept is there, but 23 people execute it in very different ways. 24 So, you know, I don't -- in my 25 opinion, there's not a standard approach to doing</p> <p style="text-align: center;">39</p>
<p>1 You know, talking with, you know, 2 people in the company as well as if others have 3 assessed the same sort of, you know, either 4 program or process and, you know, determining, you 5 know, the degree of which, you know, in an 6 assessment, you know, that -- if we're looking at 7 a control or a control structure, that, you know, 8 that's in place in its maturity. 9 Q. Just hypothetically, you've never had 10 a situation where a company said, we follow such 11 and such password policy, and then you went in, 12 looked under the hood, and they weren't actually 13 following that policy? 14 A. I'm just trying to think of -- you 15 know, I definitely had instances where, you know, 16 you see a, you know, small number of violations in 17 a large organization, right? 18 I mean, that's natural, and it's 19 actually good that you're doing an assessment in 20 order to determine, you know, whether the 21 implementation all the way down to humans who make 22 errors are doing things in a -- you know, in a 23 situation. 24 You know, it is very rare, and I'm 25 trying to, you know, rack my brain to see that an</p> <p style="text-align: center;">38</p>	<p>1 this. There's a call-out to do it. 2 Q. There's a couple -- we'll get to your 3 report in a second. I promise. But there's a 4 couple instances in your report were you mention 5 SOX -- and that's all caps S-O-X -- 6 A. Yeah. 7 Q. -- audits. 8 Do you personally have any experience 9 with SOX audits? 10 MR. TURNER: Object to form. 11 You're asking whether he's done them 12 or had experience. 13 MR. CARNEY: Involvement whether he's 14 done them; involvement, any sort of experience 15 with them. 16 THE WITNESS: Yes. I -- you know, 17 again, broadly defined in terms of experience, 18 I've been, you know, in organizations including 19 JPMorgan that have undergone SOX audits. 20 And I've, you know, reviewed them many 21 times often as part of assessment processes, you 22 know, in companies just to take a look at what the 23 SOX audits show about -- you know, my focus has 24 generally been information security controls. 25 ///</p> <p style="text-align: center;">40</p>

Gregory Rattray
2/12/2025

<p>1 BY MR. CARNEY: 2 Q. In conjunction with the SOX audits, 3 have you had to make any determinations as to 4 whether particular controls related to financially 5 material systems? 6 A. I have not -- 7 MR. TURNER: Object to form. 8 THE WITNESS: Okay. 9 I have not been an auditor, so I 10 haven't, you know, made SOX audit determinations. 11 You know, again, I haven't played the auditor 12 role. 13 BY MR. CARNEY: 14 Q. Okay. Have you had any experience 15 within -- and this is capital S-O-C 2 audits? 16 A. Yes. Pretty much similar experiences. 17 You know, JPMorgan underwent SOC 2 18 audits. I've seen a lot of SOC 2 auditing reports 19 in consulting engagements just in terms of, you 20 know, what SOC 2 auditors have said about control 21 structures and in organizations I've worked with. 22 Q. All right. 23 (Whereupon, Exhibit 1 is marked for 24 identification.) 25 ///</p> <p style="text-align: center;">41</p>	<p>1 A. Yes. 2 Q. Okay. 3 A. Yes, December 30, 2024. 4 Q. Right. 5 A. Yeah. 6 Q. And so this was a corrected report, if 7 you will, that made some sort of minor 8 typographical corrections to your earlier report; 9 is that right? 10 A. That's what I remember as well. 11 Q. Okay. And so unfortunately, that 12 report didn't have the same appendices to it, so 13 I've handed you what's been marked as Exhibit 2, 14 which has your appendices with your documents 15 reviewed, your CV and your prior testimony. 16 MR. TURNER: We would have been happy 17 to attach the same attachments, for the future. 18 Happy to send you something like that. 19 MR. CARNEY: Not a big deal. 20 MR. TURNER: Okay. 21 MR. CARNEY: There's no... 22 MR. TURNER: Killed a few trees in the 23 process. 24 MR. CARNEY: Yeah. 25 ///</p> <p style="text-align: center;">43</p>
<p>1 (Whereupon, Exhibit 2 is marked for 2 identification.) 3 MR. CARNEY: The shorter one is 4 Number 1. The bigger one is Number 2. Here's 5 Number 2. I might have another copy if you... 6 MR. TURNER: No, that's fine. I've 7 seen it before. 8 THE WITNESS: I assume I'm not allowed 9 to write on these? 10 MR. TURNER: I'm just going to put the 11 exhibit number on them. 12 THE WITNESS: Okay. 13 BY MR. CARNEY: 14 Q. All right. Dr. Rattray, I've handed 15 you what the court reporter has marked as Rattray 16 Exhibits 1 and 2. 17 A. Uh-huh. 18 Q. And just for the record, Exhibit 1 -- 19 and you can confirm this for me -- if you look at 20 the back, the last page, it should have a 21 December 30, 2024, date; is that right? 22 A. The last page of the main report? 23 Q. The last page of the entire document. 24 A. Oh, the entire document? 25 Q. Yeah.</p> <p style="text-align: center;">42</p>	<p>1 BY MR. CARNEY: 2 Q. So is it fair to say then, to 3 Mr. Turner's point, that the appendices in your 4 original report from November would be the same 5 appendices that would be attached to Exhibit 1? 6 A. Yeah, as I remember reviewing the 7 minor revisions, I didn't see anything when I 8 reviewed them that would have indicated a change 9 in any of the attachments from the original 10 report. 11 Q. Okay. Great. 12 So let's focus on Exhibit 1 for the 13 moment. 14 Have you finished all the work that 15 you were assigned to do in this case? 16 A. You know, I believe I have the right 17 if I receive new evidence to augment. I don't 18 have any current plans to do so. 19 Q. Okay. Did you yourself write 20 Exhibit 1, your expert report? 21 MR. TURNER: Object to form. 22 THE WITNESS: I wrote the report. 23 And, you know, with the -- you know, with the 24 assistance and, you know, collaboration with the 25 law firm, Latham -- Latham & Watkins.</p> <p style="text-align: center;">44</p>

Gregory Rattray
2/12/2025

<p>1 BY MR. CARNEY: 2 Q. And aside from Latham & Watkins, did 3 anyone else help you write your report? 4 A. I had research assistants from -- 5 analysts from my consulting firm, but they did not 6 write any of the report. 7 Q. And who were those research 8 assistants? 9 A. Helen Lee. 10 Q. Okay. And do you know what Ms. Lee's 11 background is? 12 A. I do. 13 Q. And what is it? 14 A. She's a graduate of Columbia 15 University, and it -- has a master's degree with a 16 focus on cybersecurity from the School of 17 International and Public Affairs and has been an 18 employee in my consulting group Next Peak. 19 Q. So she's an employee of Next Peak? 20 A. Yes. 21 Q. And besides Ms. Lee, did anyone else 22 help you? 23 A. No. 24 Q. Okay. Did anyone from SolarWinds help 25 you write this report?</p> <p style="text-align: center;">45</p>	<p>1 Q. And when you say "logging data," is 2 that related to access controls? 3 A. It may be related -- we should look at 4 the specifics. 5 Q. Okay. 6 A. You know, it may be access controls. 7 It may be, you know, firewall -- the use of 8 firewall. But we can look into the specifics in 9 the report. 10 Q. Okay. And are all of the opinions 11 you're offering in this case set forth in this 12 report, Exhibit 1? 13 A. You know, as of today, yes. 14 Q. And as of today, you said, I think, 15 you don't plan to offer any additional opinions? 16 A. That's -- 17 MR. TURNER: Objection. 18 (Pause in testimony.) 19 THE STENOGRAPHER: I don't have a full 20 answer. 21 THE WITNESS: You know, as I answered 22 previously, I don't have any current plans to 23 revise this report. 24 BY MR. CARNEY: 25 Q. Okay. And if you could just briefly</p> <p style="text-align: center;">47</p>
<p>1 A. No. 2 Q. I don't want you to tell me the 3 substance of it. Your communications with counsel 4 are covered by the work product, Rule 26. 5 But did you -- did counsel provide 6 comments to you on your drafts of this report? 7 A. Yes. 8 Q. And did you incorporate some of those 9 comments? 10 MR. TURNER: I'm just going to object 11 to the questions in terms of starting to get into 12 the details of the drafting process. 13 MR. CARNEY: Okay. 14 BY MR. CARNEY: 15 Q. I don't want to get into the details 16 of the drafting process. But I'm just trying to 17 understand how this came about. 18 Did -- you're familiar with Tim Brown, 19 right? 20 A. I am. 21 Q. Did he provide any comments or 22 suggestions to your draft reports? 23 A. I had one conversation with Tim about 24 specifics on how, you know, his practice reviewed 25 logging data. He did not comment on the report.</p> <p style="text-align: center;">46</p>	<p>1 look at Exhibit 2. And, actually, it might be 2 helpful that we have it as two separate exhibits, 3 because you can look at them side by side. 4 If you look at Appendix A to 5 Exhibit 2, is that a copy of your CV? 6 A. Yes, it is. 7 Q. And is this -- I'm not going to ask 8 you to review the whole thing, but as far as you 9 know it, does this accurately reflect your 10 education and experience? 11 A. I believe it does. 12 Q. And you've served as an expert in a 13 couple other cases; is that right? 14 A. That's correct. 15 Q. And how many -- was it two? 16 A. It's two, yeah. 17 Q. Okay. And has your expert testimony 18 ever been excluded in whole or in part by a Court? 19 A. No. 20 Q. Has the Court ever imposed any kind of 21 limitations on your ability to offer your expert 22 opinions? 23 A. No. 24 Q. In the course of serving as an expert 25 witness, has opponent ever filed a Daubert motion</p> <p style="text-align: center;">48</p>

Gregory Rattray
2/12/2025

<p>1 against you?</p> <p>2 A. Not to my knowledge.</p> <p>3 Q. And we talked a little bit about</p> <p>4 your -- you know, your arrangement here, but can</p> <p>5 you just describe to me how did you become -- come</p> <p>6 to be retained as an expert in this case? Who</p> <p>7 contacted you?</p> <p>8 THE WITNESS: I believe, Serrin, it</p> <p>9 was you. But it was definitely from Latham &</p> <p>10 Watkins.</p> <p>11 BY MR. CARNEY:</p> <p>12 Q. And had you ever worked with</p> <p>13 Mr. Turner before this case?</p> <p>14 A. I had not.</p> <p>15 Q. And do you know how he got your name</p> <p>16 or who referred you to him?</p> <p>17 A. I don't know how he got my name.</p> <p>18 Q. Man of mystery.</p> <p>19 A. I mean, again --</p> <p>20 Q. Yeah.</p> <p>21 A. -- I don't know.</p> <p>22 MR. TURNER: He has a reputation in</p> <p>23 this space. What can I tell you?</p> <p>24 MR. CARNEY: All right.</p> <p>25 ///</p> <p style="text-align: center;">49</p>	<p>1 is 10:44 a.m.</p> <p>2 We're back on the record.</p> <p>3 BY MR. CARNEY:</p> <p>4 Q. Okay. Dr. Rattray, before we broke,</p> <p>5 you had mentioned that you had some familiarity</p> <p>6 with the SEC's case against SolarWinds before you</p> <p>7 became personally involved in the case; is that</p> <p>8 right?</p> <p>9 A. That's right.</p> <p>10 Q. And how did you acquire that</p> <p>11 knowledge?</p> <p>12 A. You know, in my field, you know, in</p> <p>13 what I do, you know, you're reading news related</p> <p>14 to cybersecurity.</p> <p>15 So the SEC action, and I forget the</p> <p>16 sort of specific legal terminology around the</p> <p>17 action, but sort of the original, you know,</p> <p>18 publicly known investigation, you know, I was just</p> <p>19 reading reporting on that.</p> <p>20 Q. Okay. And were you familiar with what</p> <p>21 was known as the Sunburst incident?</p> <p>22 A. Yes, I am. Yes, I am.</p> <p>23 Q. Okay. And did you write any articles</p> <p>24 on that, do you recall?</p> <p>25 A. No. I did not, that I can recall.</p> <p style="text-align: center;">51</p>
<p>1 BY MR. CARNEY:</p> <p>2 Q. Okay. Prior to your retention, did</p> <p>3 you know anything about the SEC's case against</p> <p>4 SolarWinds?</p> <p>5 A. Yes. I was aware that -- I'm trying</p> <p>6 to remember if the case had been filed, but I was</p> <p>7 aware that there was, you know, activity between</p> <p>8 the SEC and SolarWinds.</p> <p>9 Q. Okay. Did you recall when you were</p> <p>10 retained on this case?</p> <p>11 A. I believe it was about October -- I</p> <p>12 don't want to be held to the month -- of 2023.</p> <p>13 MR. TURNER: Chris, whenever you have</p> <p>14 a moment, we've been going for about an hour.</p> <p>15 Take a break.</p> <p>16 MR. CARNEY: Sure. We can take a</p> <p>17 break now. Want to take?</p> <p>18 MR. TURNER: Yeah, thanks.</p> <p>19 MR. CARNEY: 10 minutes?</p> <p>20 THE VIDEOGRAPHER: The time right now</p> <p>21 is 10:32 a.m.</p> <p>22 We are off the record.</p> <p>23 (Whereupon, a recess was taken at</p> <p>24 10:32 a.m.)</p> <p>25 THE VIDEOGRAPHER: The time right now</p> <p style="text-align: center;">50</p>	<p>1 Q. And I'll remind you this: When I'm</p> <p>2 asking you this question, I understand you're not</p> <p>3 a lawyer. I'm not asking you for legal opinions</p> <p>4 or conclusions, but what is your understanding as</p> <p>5 to the basis of the SEC's case against SolarWinds</p> <p>6 and Tim Brown, as we sit here today?</p> <p>7 MR. TURNER: Object to form.</p> <p>8 THE WITNESS: You know, again, with</p> <p>9 your disclaimer, like, I'm not a lawyer and, you</p> <p>10 know, I'm not trying to offer legal opinion, you</p> <p>11 know, my understanding is the SEC is asserting</p> <p>12 that, you know -- assertions in the security</p> <p>13 statement are potentially fraudulent, because</p> <p>14 SolarWinds and Tim Brown, you know, knew that the</p> <p>15 state of their security was not -- not in line</p> <p>16 with what was, you know, said in the security</p> <p>17 statement.</p> <p>18 BY MR. CARNEY:</p> <p>19 Q. Okay. And once again, setting aside</p> <p>20 legal requirements, as a cybersecurity</p> <p>21 professional, do you believe it's important for</p> <p>22 companies and individuals to be truthful when</p> <p>23 making statements about their cybersecurity</p> <p>24 practices?</p> <p>25 A. Yes, I do.</p> <p style="text-align: center;">52</p>

<p>1 Q. And why do you believe that?</p> <p>2 A. You know, in general, you know,</p> <p>3 cybersecurity is a complex, challenging field.</p> <p>4 And, you know, in -- our ability to pursue it, you</p> <p>5 know, needs to be based on, you know, good</p> <p>6 information that we need to trust that when we're</p> <p>7 communicating with each other, that, you know, to</p> <p>8 the best of an individual's, you know, ability,</p> <p>9 that they're representing things accurately.</p> <p>10 Q. And if I could ask you, sir, to turn</p> <p>11 to paragraph 13 of Exhibit 1.</p> <p>12 And you can read that whole paragraph</p> <p>13 to yourself if you want, but --</p> <p>14 A. Oh, sorry. I turned to page 13.</p> <p>15 Q. I'm sorry. Page 5, paragraph 13.</p> <p>16 MR. TURNER: Which one are we on?</p> <p>17 Exhibit 1 or Exhibit 2?</p> <p>18 MR. CARNEY: Exhibit 1. Thank you.</p> <p>19 THE WITNESS: Yes. I've read it.</p> <p>20 BY MR. CARNEY:</p> <p>21 Q. And in the third sentence, you say, "I</p> <p>22 understand that the Securities & Exchange</p> <p>23 Commission (SEC) has alleged that these</p> <p>24 representations were false or misleading during</p> <p>25 the time period from SolarWinds's initial public</p> <p>53</p>	<p>1 Would that be, in your view, a</p> <p>2 misstatement?</p> <p>3 MR. TURNER: Object to form.</p> <p>4 THE WITNESS: You know, I don't know</p> <p>5 that -- I think in that particular set of</p> <p>6 hypothetical circumstances, you know, I think</p> <p>7 you'd have to go deeper and, you know -- does it</p> <p>8 cover 99 percent of the period? Did it cover</p> <p>9 2 percent of the period?</p> <p>10 Again --</p> <p>11 BY MR. CARNEY:</p> <p>12 Q. Let's say --</p> <p>13 A. -- no --</p> <p>14 Q. All right. I'll change my</p> <p>15 hypothetical then to fit that then.</p> <p>16 A. Okay.</p> <p>17 Q. Let's say instead of it being from --</p> <p>18 the policy being -- follow from October of 2018 to</p> <p>19 January of 2021, it was followed from October of</p> <p>20 2018 to October of 2019, would that be a</p> <p>21 misleading statement if they said they followed it</p> <p>22 for that entire period?</p> <p>23 MR. TURNER: Object to form without</p> <p>24 more specifics.</p> <p>25 THE WITNESS: Again, we're talking</p> <p>55</p>
<p>1 offering which occurred on October 19, 2018, to</p> <p>2 January 12, 2021."</p> <p>3 And you refer to that as the relevant</p> <p>4 period.</p> <p>5 Once again, not asking for a legal</p> <p>6 opinion, but what is your understanding as to what</p> <p>7 it means for a representation to be false or</p> <p>8 misleading as you use that term in this sentence?</p> <p>9 A. Yeah, I'm not quite sure how I can --</p> <p>10 you know, I could reframe words, but to me, those</p> <p>11 are pretty -- you know, do you want me to define</p> <p>12 what's a falsehood?</p> <p>13 Q. And fair question. I'm just trying to</p> <p>14 understand your use of the term, so let me give</p> <p>15 you a -- try to give you a hypothetical. And once</p> <p>16 again, this is a hypothetical. I'm not saying</p> <p>17 this is SolarWinds's here.</p> <p>18 But let's say you refer to a time</p> <p>19 period October of 2018 to January of 2021. Let's</p> <p>20 say that they -- a company said they were</p> <p>21 following certain cybersecurity practices during</p> <p>22 that period --</p> <p>23 A. Yes.</p> <p>24 Q. -- but they're only following it for a</p> <p>25 short amount of that period.</p> <p>54</p>	<p>1 about, again, in this case, the company saying</p> <p>2 something -- you know, they -- they performed --</p> <p>3 you know, they said they performed a practice and</p> <p>4 they only performed it for half the time of a</p> <p>5 period --</p> <p>6 BY MR. CARNEY:</p> <p>7 Q. Yes.</p> <p>8 A. -- I just want to make sure I'm</p> <p>9 understanding.</p> <p>10 You know, in terms of that being false</p> <p>11 or misleading, I think it would have to link to</p> <p>12 whether the company -- the company had represented</p> <p>13 they were following it for the full period or not,</p> <p>14 right, you know.</p> <p>15 Q. Okay.</p> <p>16 A. Yeah.</p> <p>17 Q. So my hypothetical was they said,</p> <p>18 we're doing this, let's say it's strong access</p> <p>19 controls for this entire period, but it turned out</p> <p>20 they were only doing it for that year.</p> <p>21 And I'm just trying to make the</p> <p>22 hypothetical as simple as possible.</p> <p>23 MR. TURNER: Object to form. Object</p> <p>24 to the term "strong."</p> <p>25 THE WITNESS: Yeah, I actually think,</p> <p>56</p>

Gregory Rattray
2/12/2025

1 you know, not being a lawyer and not, you know,
2 understanding what, you know, is defined as false
3 or misleading -- right? -- and my job was to just,
4 you know, look at the presence, you know,
5 basically were they doing what they represented.
6 So we might come back to this.

7 But, like, in determining whether
8 something is false or misleading probably wasn't
9 in the scope for me. It was -- I was trying to
10 determine what -- what they said in the statement,
11 were they doing it, which in all cases of things I
12 examined, they were.

13 BY MR. CARNEY:

14 Q. Okay. I'll change my hypothetical to
15 match that then.

16 Let's say the company said, we have a
17 complex password policy that we followed from
18 October of 2018 to January of 2021.

19 Do you follow that so far?

20 A. Yeah. Hypothetical that the company
21 said they had a complex password policy during
22 that period.

23 Q. Okay.

24 MR. TURNER: Object to form.

25 ///

57

1 A. You know, to the extent to which --
2 you know, I'd have to understand the context
3 around the email, whether it was an authoritative
4 statement, you know, to the company.

5 I mean, yeah, so if -- you know, if
6 they -- if they said they were doing something and
7 then, you know -- and in a -- you know, provably
8 factual way they said they stopped doing it during
9 the period but continued to represent that they
10 were -- I mean, in some ways it just goes --
11 revolves around to if they were saying they were
12 doing it during a period and they, you know, had
13 said that they weren't doing it in the same
14 period, you know, that probably seems to be a
15 misrepresentation.

16 Q. Okay. Prior to your retention by
17 SolarWinds via Latham & Watkins, had you ever
18 discussed this case with any SolarWinds employee?

19 A. No.

20 Q. Aside from your work on this case,
21 have you ever done any other work for SolarWinds?

22 A. No.

23 Q. So you've never consulted on
24 cybersecurity issues for SolarWinds apart from
25 this case?

59

1 BY MR. CARNEY:

2 Q. And then but in actuality after a
3 year, they just completely stopped enforcing that
4 password policy in 2019.

5 Would that statement, in your view,
6 not a legal view, be incorrectly describing their
7 cybersecurity practices?

8 A. I just want to make sure I understand,
9 you know. Is the question whether they, you know,
10 misrepresented on having a policy, or is it a
11 question -- a question of if they stopped -- you
12 used the word "enforcement" in the middle of the
13 period, you know, did they -- I'd have to look at
14 the actual written statement to make a
15 determination of misrepresentation if, you know,
16 they had a policy and then the details around what
17 constituted the drop-off in enforcement to make a
18 determination around this misrepresentation.

19 Q. All right. Fair enough. I'll adjust
20 the hypothetical to address that.

21 Let's say after the year, company --
22 internal email memo said, we are no longer -- have
23 this policy, this complex password policy from now
24 on, but they represented to the public that they
25 had it for the entire 2.5 year period.

58

1 A. That's correct.

2 Q. Prior to your work on this case, have
3 you ever done any work for Latham & Watkins?

4 A. No.

5 Q. And I think it's in your report, but
6 do you recall what your hourly rate is for this
7 case?

8 A. It's \$1,100 an hour.

9 Q. Okay. And I think you said that you
10 personally billed about 200 hours; is that right?

11 A. Yeah. Again, I have not looked at
12 each of the invoices over the period. I think
13 that's in the ballpark, but it might be a big
14 ballpark.

15 Q. And was it -- was it Ms. Lee that you
16 said also worked on the case with you?

17 A. That's right.

18 Q. And do you know how many hours she's
19 billed?

20 A. I don't know how many hours she's
21 billed.

22 Q. Just quickly, did do you anything to
23 prepare for the deposition today?

24 A. Yes, I did.

25 Q. And what did you do?

60

Gregory Rattray
2/12/2025

<p>1 A. I primarily reviewed my report and 2 Mr. Graff's report, you know, some of the 3 documentation that was cited in both reports, I 4 had discussions with the Latham team. 5 Q. Okay. Did you meet with the Latham 6 team in preparation for your deposition? 7 A. Yes, I did. 8 Q. And how many times did you meet with 9 them? 10 A. I would say probably three sessions 11 focused on this deposition. 12 Q. Okay. And were those sessions in 13 person? 14 A. I was here Monday afternoon and 15 yesterday. So two of those -- you know, two of 16 those were in person. 17 Q. Okay. Did you speak with anyone else 18 other than counsel in preparation for your 19 deposition? 20 A. No. 21 Q. And so how long did you meet with 22 defense counsel in total to prepare for your 23 deposition would you say in terms of hours? 24 A. Meet with counsel? You know, I would 25 say -- again, focused on the deposition --</p> <p style="text-align: center;">61</p>	<p>1 A. I -- 2 MR. TURNER: Object to form. 3 THE WITNESS: Yeah. 4 MR. TURNER: And object to getting 5 into any conversations with counsel about that. 6 BY MR. CARNEY: 7 Q. Yeah. I don't want to get into any 8 conversations. I want to understand what the 9 process by which you received these documents 10 were. 11 Did you choose them? Did they choose 12 them? How did that come about? 13 MR. TURNER: Do you want to ask more 14 generally about the types of documents he was 15 interested in reviewing? 16 BY MR. CARNEY: 17 Q. I guess I want to understand, did you 18 have a role in selecting what documents you looked 19 at, or did someone else select them for you? 20 MR. TURNER: Object to the form. 21 "Select." 22 THE WITNESS: Proceed? 23 MR. TURNER: Yes, you can. 24 THE WITNESS: Yes, I did have a role 25 in that.</p> <p style="text-align: center;">63</p>
<p>1 right? -- 10, 12 -- between 10 and 15 hours maybe. 2 Q. All right. Sir, I want to ask you 3 now -- and I'm going to ask you on Exhibit 2, you 4 have an Appendix C at the back. It's the -- I 5 think it's the last appendix -- 6 A. Yep. 7 Q. -- list of materials you considered in 8 preparing your report. 9 And did you personally review each of 10 the materials listed in Appendix C? 11 A. Yes, I did. 12 Q. And over what time period did you 13 review all of those materials? 14 A. You know, there's materials, you know, 15 that I received during the course of this. A 16 large amount of the materials, but particularly 17 what I call these tranches of data about the 18 presence of controls, you know, I really only 19 reviewed in October and November of this past 20 fall. So October and November of 2024. 21 But, again, I had access to some of 22 the documents cited from earlier -- you know, 23 earlier in the proceeding. 24 Q. Okay. Did counsel choose the 25 documents for you to look at?</p> <p style="text-align: center;">62</p>	<p>1 BY MR. CARNEY: 2 Q. And what was your role? 3 A. You know, as I was conducting my, you 4 know, work, I wanted -- I requested to see, you 5 know, documentation, you know, particularly around 6 the implementation of practices and controls. 7 Q. Okay. Did you provide counsel with 8 search terms to use in looking for documents? 9 A. You know, to the extent to which I 10 gave language around -- around the types of 11 controls that I was looking for, evidence, you 12 know, of practice, I don't know if we call those 13 search terms or not, but I definitely used 14 language to communicate to them what I was looking 15 for. 16 Q. Did you have a keyword list that 17 you -- 18 MR. TURNER: I'll object to form. 19 These are conversations with counsel. 20 I can represent that the witness asked for various 21 types of documents related to the security domains 22 at issue, and SolarWinds tried to provide 23 documents that were responsive to those requests. 24 BY MR. CARNEY: 25 Q. And so Solar -- did you have any</p> <p style="text-align: center;">64</p>

1 communications directly with SolarWinds about the
2 documents that you wanted?

3 **A.** I had conversations with SolarWinds,
4 two short conversations with SolarWinds people
5 about questions I had upon looking at the
6 documents. I did not -- I did not request
7 directly from SolarWinds documentation.

8 **Q.** Okay. And were those conversations
9 with Mr. Brown and Mr. Kline?

10 **A.** That's correct.

11 **Q.** Okay. So, first of all, the
12 conversation with Mr. Brown, what did you discuss
13 with him?

14 **A.** Again, in both cases, I was just
15 trying to understand some of the more detailed,
16 you know, documentation and how the teams that
17 they were responsible for, you know -- you know,
18 worked with that documentation logging data and
19 those sorts of things.

20 **Q.** And were those conversations over the
21 phone?

22 **A.** I'm trying to remember if they were
23 Zoom or phone or -- they were remote
24 conversations.

25 **Q.** Okay. And were they separate

65

1 very familiar with how such assessments are
2 ordinarily done.

3 "An outside expert assessing whether a
4 company has certain controls in place gathers
5 information from people in the company who are
6 knowledgeable about the controls in order to
7 understand how they are designed and looks for
8 artifacts generated from the operation of those
9 controls to ensure that they were implemented."

10 So I want to ask you about that.

11 **A.** Uh-huh.

12 **Q.** In this case, you were in 2024 trying
13 to assess whether SolarWinds had certain controls
14 in place during what you described as the relevant
15 period of October of 2018 to January of 2021,
16 right?

17 **A.** That's correct.

18 **Q.** Prior to this case, have you ever
19 previously been asked to assess whether a company
20 had cyber -- cybersecurity controls in place years
21 earlier than the time at which you were conducting
22 your assessment?

23 **A.** Yes.

24 **Q.** And when was that?

25 **A.** Certainly in the matter that's listed

67

1 conversations, your conversation with Mr. Brown
2 and with Mr. Kline?

3 **A.** Yes, they were.

4 **Q.** And do you recall when those
5 conversations took place?

6 **A.** Not specifically. I believe it
7 probably was November '24.

8 **Q.** Okay. And was it just you and
9 Mr. Brown on the call, or were counsel on the call
10 as well?

11 **A.** Counsel was on the call.

12 **Q.** In preparing your opinions set forth
13 in Exhibit 1, did you consider any sources not
14 cited in Exhibit 1 in Appendix C?

15 **A.** Can you just sort of restate that?

16 **Q.** Sure.

17 **A.** I just want to make sure I get the
18 causality.

19 **Q.** Yeah. All I'm getting at is, are
20 there documents that aren't sort of reflected or
21 described in your report?

22 **A.** No, I don't think so.

23 **Q.** Okay. On page 1 of Exhibit 1,
24 paragraph 2, you say, "Having conducted or
25 overseen numerous cybersecurity assessments, I'm

66

1 where I was an expert, the Insulet case. That was
2 the situation there as well.

3 **Q.** And what was the situation in the
4 Insulet case?

5 **A.** The Insulet case was a trade secret
6 matter, and so it was the plaintiff. And the
7 defendants -- there were questions by the
8 defendants about the presence of reasonable
9 measures that, you know -- in place at Insulet.

10 And, you know, my -- my role was to
11 assess whether those information security measures
12 were in place.

13 **Q.** And were you an expert for the
14 defendant in that case?

15 **A.** No. I was an expert for the plaintiff
16 Insulet.

17 **Q.** For Insulet.

18 And you were assessing whether the
19 controls that they said they had in place to
20 protect the trade secrets were actually there?

21 **A.** Yeah. I mean, you know, in trade
22 secret cases, you know, the language, I believe,
23 is -- not being a lawyer -- is reasonable
24 measures. So, you know, my -- my expert opinion,
25 you know, talked to the measures they had and

68

Gregory Rattray
2/12/2025

1 their information security practice.

2 **Q.** Okay. And in that case, were you
3 looking at the policies that Insulet had in place,
4 or were you also looking at the artifacts showing
5 the implementation of those policies?

6 **A.** Both.

7 **Q.** And how many years earlier were you
8 looking from when you were offering your
9 assessment?

10 **A.** Many. You know, from -- as -- you
11 know, even earlier to a degree, but probably would
12 call the start date 2007 and -- to about 2014 --
13 that was the period where, you know -- that was
14 the focus.

15 Though -- the case did -- did require
16 me to look post-2015, effectively up to the
17 present day. But the focus was in that earlier
18 period.

19 **Q.** And did you testify at trial in that
20 case?

21 **A.** I did.

22 **Q.** And what was the result of that case?

23 **A.** Insulet won that case.

24 **Q.** Now, sir, in paragraph 3, the first
25 sentence is -- you say, "Applied these standard

69

1 practices in assessing whether SolarWinds
2 implemented the practices at issue in the
3 securities statement."

4 So my question for you is: What are
5 the standard practices in conducting an assessment
6 as to whether a company employed cybersecurity
7 practices years earlier than the time you're
8 looking at?

9 MR. TURNER: Object to form.

10 THE WITNESS: You know, in my opinion,
11 you know, having, again, done it in the one case,
12 but in almost all assessments, you're looking to
13 some degree into the past, right? You know, in
14 terms of -- you know, the presence of policies,
15 some of which can be -- have been in place for
16 years.

17 So I guess is the question about is
18 there a distinction between the methodology for
19 past situations and current situations, or just
20 was is the standard methodology?

21 **Q.** Yeah, so why don't we do both.

22 **A.** Okay.

23 **Q.** Why don't we say what is the standard
24 methodology, and then you can tell me if there's a
25 difference.

70

1 **A.** Okay. Yes. So if -- I'll answer the
2 second question first, there's not really a
3 difference, right, you know?

4 **Q.** Okay.

5 **A.** So in terms of, you know, how one
6 conducts an assessment, you know, you are looking
7 for, you know, the presence of policy and
8 procedure. You know, evidence that managers, you
9 know, are -- you know, are running those policies
10 and procedures.

11 Could be through interviews, in the
12 case of SolarWinds, this case, significant
13 testimony through depositions.

14 And then, you know, artifacts showing
15 those practices and implementation as well as
16 looking at, if it's available, other outside
17 assessments, you know, that are -- you know, sort
18 of who are -- have also been conducted such as
19 we've discussed, the Sarbanes-Oxley and the SOC 2
20 audits.

21 So my -- you know, my approach to this
22 practice or what I believe to be standard practice
23 is using those sets of evidence to assess whether
24 the practice is in place.

25 **Q.** All right. And I just want to sort of

71

1 backtrack to something that I asked you about
2 before the break.

3 You're not an accountant, right?

4 **A.** I'm not. I don't hold a certified
5 public accounting certification, no.

6 **Q.** And you don't have expertise as to
7 whether a statement is material within the meaning
8 of GAAP, right?

9 MR. TURNER: Object to form.

10 THE WITNESS: Yeah, and I assume GAAP,
11 you're talking about generally accepted accounting
12 principles?

13 BY MR. CARNEY:

14 **Q.** Right.

15 **A.** Can you repeat the question?

16 **Q.** Sure.

17 You don't have expertise in whether a
18 statement is material within the meaning of GAAP,
19 right?

20 **A.** No.

21 **Q.** Okay. And you don't have -- profess
22 to have expertise as to whether an accountant, a
23 CPA would find a statement to be misleading under
24 GAAP, right?

25 MR. TURNER: Object to form.

72

Gregory Rattray
2/12/2025

<p>1 THE WITNESS: Yeah, I don't.</p> <p>2 BY MR. CARNEY:</p> <p>3 Q. Okay. All right. Let me ask you,</p> <p>4 paragraph 4, which is on page 2, you say -- with</p> <p>5 regards to Mr. Graff's report, there's a statement</p> <p>6 down in sort of the middle of the paragraph, you</p> <p>7 say, "The documents he cites generally have little</p> <p>8 to do with the practices described in the security</p> <p>9 statement, et al."</p> <p>10 What does that mean?</p> <p>11 A. Generally -- right? -- you know, I</p> <p>12 found that some -- you know, the documents such as</p> <p>13 some of the emails and PowerPoint documents, you</p> <p>14 know, were not direct evidence of whether the</p> <p>15 practices in the securities statement were in</p> <p>16 place.</p> <p>17 Q. But when you say they have little to</p> <p>18 do with the practices, are you saying they're just</p> <p>19 completely unrelated to cybersecurity at</p> <p>20 SolarWinds?</p> <p>21 MR. TURNER: Object to form.</p> <p>22 THE WITNESS: You know, this sentence,</p> <p>23 you know, is focused on the fact that those</p> <p>24 documents are not the most relevant documents</p> <p>25 related to the practices.</p> <p style="text-align: center;">73</p>	<p>1 Are you asking whether the FedRAMP</p> <p>2 assessment was an assessment of the securities</p> <p>3 statement?</p> <p>4 MR. CARNEY: No. I'm asking -- he</p> <p>5 said that the documents had little to do with the</p> <p>6 practices described in the securities statement.</p> <p>7 BY MR. CARNEY:</p> <p>8 Q. And I'm simply asking whether the</p> <p>9 FedRAMP items that were being assessed did, in</p> <p>10 fact, relate to the practices that are described</p> <p>11 in the securities statement.</p> <p>12 A. You know, I just want to make sure,</p> <p>13 because it wasn't a security assessment and, you</p> <p>14 know -- you know, it really didn't, you know, have</p> <p>15 bearing on whether SolarWinds had done the things</p> <p>16 that they said in the securities assessment,</p> <p>17 right?</p> <p>18 Yeah, I mean, again, that's why I --</p> <p>19 you know, that's an example of something that he</p> <p>20 cites that is really not, in this case, related to</p> <p>21 the security statement.</p> <p>22 Q. All right. Is there an industry</p> <p>23 standard for determining whether a company has</p> <p>24 properly employed cybersecurity practices?</p> <p>25 A. There are lots of standards about</p> <p style="text-align: center;">75</p>
<p>1 BY MR. CARNEY:</p> <p>2 Q. And what do you mean by that? When</p> <p>3 you say "practices," what do you mean?</p> <p>4 A. Things like the presence of access</p> <p>5 controls or password.</p> <p>6 Q. All right. Can you think of an</p> <p>7 example that he cites as little to do with the</p> <p>8 practices described in the securities statement?</p> <p>9 A. I mean, one would be the -- you know,</p> <p>10 the FedRAMP assessment.</p> <p>11 Q. And why does that have little to do</p> <p>12 with the practices described in the securities</p> <p>13 statement?</p> <p>14 A. Because that assessment was conducted</p> <p>15 in a quick and dirty fashion for a budgeting</p> <p>16 exercise.</p> <p>17 Q. But would you agree that the subject</p> <p>18 of the assessment related to the practices at</p> <p>19 issue in the security statement?</p> <p>20 A. Can you repeat the question?</p> <p>21 Q. Sure.</p> <p>22 Would you agree that the subject of</p> <p>23 the FedRAMP assessment related to the practices at</p> <p>24 issue in the security statement?</p> <p>25 MR. TURNER: Object to form.</p> <p style="text-align: center;">74</p>	<p>1 cybersecurity practices.</p> <p>2 Q. But is there a sort of overarching</p> <p>3 standard that's used in determining whether a</p> <p>4 company is properly employing the security --</p> <p>5 cybersecurity practices it professes to follow?</p> <p>6 MR. TURNER: Object to form.</p> <p>7 And the witness has already explained</p> <p>8 what he understood to be the standard approach to</p> <p>9 assessing that issue.</p> <p>10 THE WITNESS: Again, there are, you</p> <p>11 know, systems and frameworks, you know,</p> <p>12 promulgated by different organizations around</p> <p>13 cybersecurity. You know -- you know, my</p> <p>14 estimation is there's not one overarching singular</p> <p>15 standard.</p> <p>16 BY MR. CARNEY:</p> <p>17 Q. Okay. And I guess in a related</p> <p>18 question, so is there not -- is there a particular</p> <p>19 standard that you followed in determining whether</p> <p>20 SolarWinds employed the cybersecurity practices it</p> <p>21 professed to employ that you're saying that</p> <p>22 Mr. Graff didn't follow?</p> <p>23 A. My assessment was based on, you know,</p> <p>24 my experience in, you know, the conduct of</p> <p>25 assessments that utilize a variety of -- you know,</p> <p style="text-align: center;">76</p>

Gregory Rattray
2/12/2025

<p>1 my experience includes assessments that are done 2 under a number of different frameworks, which I've 3 cited in my report. 4 The assessment wasn't aligned to a 5 specific standard. 6 Q. All right. Now I want to get into 7 your qualifications briefly. 8 So maybe if you have -- you have 9 your -- your report, which is Exhibit 1, and then 10 Exhibit 2, we have your CV? 11 A. Uh-huh. 12 Q. If you could just open up your CV -- 13 A. Yep. 14 Q. -- that would be great. So in 15 paragraph 6, it says that you're currently a 16 partner at Next Peak LLC, a cybersecurity 17 consulting company that you cofounded in 2019; is 18 that right? 19 A. That's right. 20 Q. And then over on your CV, Exhibit 2, 21 you see it has a similar entry. 22 Do you see that? 23 A. Am I looking at two different things 24 or -- 25 Q. Yeah. So I was looking at -- side by</p> <p style="text-align: center;">77</p>	<p>1 oversight of teams. So personally conducted, I 2 have been in rooms during the conduct of 3 penetration tests and red team exercises. 4 As we've discussed, I'm not a coder, 5 and I did not launch the specific tools during -- 6 you know, during penetration testing and 7 exercises. 8 I very much read the results, the 9 outputs and, you know, been involved in the 10 determination of, you know, the data we received 11 back and how to report it to the clients. 12 Q. Okay. And you mentioned that you 13 didn't launch the specific tools. Is that 14 something you could do, though, launch the 15 specific tools for penetration testing? 16 A. Again, I'm just trying to be precise. 17 I could launch them, right? 18 I would probably not want myself to be 19 doing that, because you want people that know how 20 to use those tools and have a -- sort of 21 experience and are proficient in them, which is 22 not my expertise. 23 Q. Okay. And then it also mentions red 24 team exercises. 25 Have you personally conducted red team</p> <p style="text-align: center;">79</p>
<p>1 side, I was looking at page 2 -- 2 A. Okay. 3 Q. -- of Exhibit 1 -- 4 A. Gotcha. 5 Q. -- sorry about that. 6 A. No worries. Okay. 7 Q. And, yeah. So paragraph 6 describes 8 your work at Next Peak; is that right? 9 A. That's correct. 10 Q. And then your CV also has a similar 11 entry about that, right? 12 A. That's correct. 13 Q. And then in paragraph 6, it says -- 14 the last sentence, it says, "My teams also assist 15 our clients in conducting penetration testing and 16 red team exercises, both of which involve 17 structured testing efforts to find flaws and 18 vulnerabilities in IT defenses." 19 So have you -- I'm just trying to 20 understand how this works. Have you personally 21 ever conducted penetration testing? 22 A. I guess my -- can I ask a 23 clarification? 24 Q. Absolutely. 25 A. You know, I have had, you know,</p> <p style="text-align: center;">78</p>	<p>1 exercises? 2 MR. TURNER: Object to form. 3 THE WITNESS: Again, I mean, I think 4 I've answered that in the sense that it -- what I 5 said about being physically present -- you know, 6 designing the exercises, being physically present 7 during their execution. Being part of the team 8 that decided, you know, what we saw in -- you 9 know, and discussed -- you know. 10 To me that's participation at a deep 11 level in the conduct of the exercise. 12 BY MR. CARNEY: 13 Q. Okay. But a similar -- so, first of 14 all, do you need any certain certifications to be 15 able to conduct red team exercises? 16 A. Legally? I mean, like, required? 17 Required by whom? 18 Q. Or just from a technical standpoint. 19 A. Again, required? You used the verb 20 "required." 21 Q. Right. 22 A. I'm just trying to -- like, who's 23 requiring it? 24 Q. Could someone carry out a red team 25 exercise if they didn't have certain technical</p> <p style="text-align: center;">80</p>

Gregory Rattray
2/12/2025

<p>1 certifications?</p> <p>2 A. I wouldn't advise that, but it's</p> <p>3 legally permissible.</p> <p>4 Q. Okay. And what type of certifications</p> <p>5 does someone have who's conducting a red team</p> <p>6 exercise?</p> <p>7 A. There are certifications -- well,</p> <p>8 again, the conduct involves many people, you know,</p> <p>9 in terms of design, you know, oversight, you know,</p> <p>10 technical activity, you know, analysis and</p> <p>11 reporting.</p> <p>12 So, you know, different certifications</p> <p>13 are probably applicable to different -- to</p> <p>14 different activities and different qualifications</p> <p>15 exist across that set of things that, you know,</p> <p>16 are inherent in the conduct of a red team exercise</p> <p>17 or a pen test.</p> <p>18 Q. Have you taken any formal training in</p> <p>19 pen tests?</p> <p>20 A. Formal training, I have not undertaken</p> <p>21 any formal training.</p> <p>22 Q. All right. Let me move on to the next</p> <p>23 paragraph. It says, "Additionally, I am the chief</p> <p>24 strategy and risk officer for Andesite AI, early</p> <p>25 stage company focused on the improvement of</p> <p style="text-align: center;">81</p>	<p>1 everything from market opportunity to, you know,</p> <p>2 the direction of the product.</p> <p>3 Q. How do you split your time between</p> <p>4 Next Peak and Andesite, 50/50 or more at one?</p> <p>5 A. It's probably close to 50/50. You</p> <p>6 know, it very much varies from week to week.</p> <p>7 Q. Okay. All right. Okay. If we move</p> <p>8 on to paragraph 8, it says, "From 2014 to 2019, I</p> <p>9 was chief information security officer and head of</p> <p>10 global cyber partnerships at JPMorganChase where I</p> <p>11 directed its cyber defense program and oversaw</p> <p>12 more than a thousand personnel in a \$500 million</p> <p>13 budget."</p> <p>14 And if we look over in Exhibit 2 on</p> <p>15 A-2, second page of your CV, it also says, "chief</p> <p>16 information security officer and head of global</p> <p>17 cyber partnerships 2014 to 2019"; is that right?</p> <p>18 A. That is right.</p> <p>19 Q. So let me break that down.</p> <p>20 So from 2014 to 2019, you were what</p> <p>21 was called the CISO at JPMorganChase?</p> <p>22 A. I was the CISO for a year, 2014 to</p> <p>23 2015, and then I was asked to take a broader role</p> <p>24 as the head of global cyber partnerships.</p> <p>25 Q. So on your resumé, on your CV, and in</p> <p style="text-align: center;">83</p>
<p>1 cybersecurity operations through advanced data</p> <p>2 science and artificial intelligence."</p> <p>3 So -- and looks -- if you look at your</p> <p>4 CV next to it, it says 2023 to the present.</p> <p>5 So you've had both these jobs at</p> <p>6 Andesite and Next Peak at the same time?</p> <p>7 A. That's correct.</p> <p>8 Q. And do you collect a salary from</p> <p>9 Andesite?</p> <p>10 A. Yes, I do.</p> <p>11 Q. Okay. Are you an owner of Andesite?</p> <p>12 A. I have a small amount of equity in</p> <p>13 Andesite.</p> <p>14 Q. And what are --</p> <p>15 A. Actually, they're options. So they</p> <p>16 haven't been exercised yet.</p> <p>17 Q. And is Andesite publicly traded?</p> <p>18 A. No.</p> <p>19 Q. I guess it says right there.</p> <p>20 What are your responsibilities at</p> <p>21 Andesite?</p> <p>22 A. I'm on the senior management team.</p> <p>23 You know, again as -- primarily as the chief</p> <p>24 strategy officer, I advise the CEO and the board</p> <p>25 on, you know, the direction of the company,</p> <p style="text-align: center;">82</p>	<p>1 the report, where it says that you were the CISO</p> <p>2 from 2014 to 2019, that's not accurate, is it?</p> <p>3 A. You know, I believe it's accurate to</p> <p>4 say that I was -- during that period, I was the</p> <p>5 chief information security and then had a role as</p> <p>6 the head of global cyber partnerships.</p> <p>7 Q. Okay. The second part of the first</p> <p>8 sentence in paragraph 8 where it says, "Where I</p> <p>9 directed its cyber defense program," that's the</p> <p>10 responsibilities of the CISO -- right? -- to</p> <p>11 direct the cyber defense program?</p> <p>12 A. It is the -- you know, the</p> <p>13 responsibility of the -- the team that CISO is the</p> <p>14 senior director. I would agree with that.</p> <p>15 Q. Okay. And a CISO is the one that</p> <p>16 directs the cyber defense program, right?</p> <p>17 A. Yeah, I mean -- yes.</p> <p>18 MR. TURNER: Are you asking at</p> <p>19 JPMorgan?</p> <p>20 MR. CARNEY: At JPMorganChase.</p> <p>21 THE WITNESS: Yeah, yeah --</p> <p>22 MR. CARNEY: Yes.</p> <p>23 THE WITNESS: -- yeah.</p> <p>24 BY MR. CARNEY:</p> <p>25 Q. So you directed the cyber defense</p> <p style="text-align: center;">84</p>

Gregory Rattray
2/12/2025

<p>1 program at JPMorgan from 2014 to 2015, right?</p> <p>2 A. That's right.</p> <p>3 Q. You didn't direct the cyber defense</p> <p>4 program at JPMorgan from 2014 to 2019, did you?</p> <p>5 A. From 2015 to 2019?</p> <p>6 Q. From 2015 to 2019.</p> <p>7 A. That's right.</p> <p>8 Q. Okay. So is it fair to say that this</p> <p>9 sentence here in your report is inaccurate?</p> <p>10 A. No. Because the sentence reads I was</p> <p>11 the chief information security officer and had</p> <p>12 global cyber partnerships, and I did direct the</p> <p>13 cyber defense program during that period.</p> <p>14 Q. But you only -- you would agree that</p> <p>15 it says from 2014 to 2019, right?</p> <p>16 A. Right.</p> <p>17 Q. And you only directed that program</p> <p>18 from 2014 to 2015; is that right?</p> <p>19 A. Right. I think it's, you know, an</p> <p>20 issue of, you know, semantic interpretation, you</p> <p>21 know, my interpretation would be that that --</p> <p>22 during that period, that was one of my duties.</p> <p>23 Q. Okay. And if we look over at your CV</p> <p>24 on page A-2, it says, "chief information security</p> <p>25 officer and head of global cyber partnerships,</p> <p style="text-align: center;">85</p>	<p>1 A. Uh-huh.</p> <p>2 Q. When you were the CISO, did you</p> <p>3 oversee more than a thousand personnel?</p> <p>4 A. Yes.</p> <p>5 Q. When you were the head of global cyber</p> <p>6 partnerships, how many personnel did you oversee?</p> <p>7 A. A much more limited, again, to my --</p> <p>8 you know, number than 1,000. Hesitant to give an</p> <p>9 exact number, because: A, it changed; and B, I</p> <p>10 have obligations to JPMorgan not to disclose --</p> <p>11 it's a pretty broad obligation not to disclose</p> <p>12 details.</p> <p>13 Q. Would it be fair to say that it was</p> <p>14 less than 10 people?</p> <p>15 A. Not necessarily, you know, yeah. At</p> <p>16 times it probably was more than 10 people.</p> <p>17 Q. Would it be fair to say that it was</p> <p>18 less than 20 people?</p> <p>19 A. Yes.</p> <p>20 Q. And when it talks about a \$500 million</p> <p>21 budget, did you oversee a \$500 million budget when</p> <p>22 you were the CISO?</p> <p>23 A. Yes. Well -- yes. You know, we were</p> <p>24 moving to a \$500 million budget in the 2015 time</p> <p>25 frame.</p> <p style="text-align: center;">87</p>
<p>1 managing director, JPMorganChase from 2014 to</p> <p>2 2019," right?</p> <p>3 A. That's correct. The same as the other</p> <p>4 document. That's correct.</p> <p>5 Q. So you would agree that on your CV, it</p> <p>6 represents that you were the CISO from 2014 to</p> <p>7 2019, right?</p> <p>8 A. No. It represents that I had two</p> <p>9 roles, the chief information security officer role</p> <p>10 and the head of global cyber partnerships role.</p> <p>11 Q. So you -- you think that someone</p> <p>12 reading your report or reading your CV would</p> <p>13 understand that you were not the CISO from 2014 to</p> <p>14 2019?</p> <p>15 A. I mean, my CV includes a -- you know,</p> <p>16 more bullets on things that were head of global</p> <p>17 cyber partnership roles than they were chief</p> <p>18 information security officer roles.</p> <p>19 So, you know, I think it's -- it's</p> <p>20 fair to say the reader would understand that some</p> <p>21 of this was CISO role and some of this was head of</p> <p>22 global cyber partnership role.</p> <p>23 Q. Okay. When -- all right. Let's focus</p> <p>24 on the second part of that sentence where it talks</p> <p>25 about more than a thousand personnel.</p> <p style="text-align: center;">86</p>	<p>1 Q. Okay. And, in fact, at the time that</p> <p>2 you left as CISO, JPMorgan's cybersecurity budget</p> <p>3 was around \$250 million; is that right?</p> <p>4 A. I don't -- I don't -- I mean: A, I'm</p> <p>5 not at liberty to say what it was. You know, and,</p> <p>6 B, I don't agree that that was the number.</p> <p>7 Q. And are you aware of public news</p> <p>8 reports that JPMorgan planned to increase its</p> <p>9 cybersecurity budget from \$250 million to</p> <p>10 \$500 million over a period of five years?</p> <p>11 A. I'm not aware of that public news</p> <p>12 report.</p> <p>13 Q. When you -- when you say that you were</p> <p>14 asked to go -- I think you described, asked to go</p> <p>15 into a broader role at the company, is it actually</p> <p>16 true that you were removed as the CISO in 2015?</p> <p>17 A. That's not true.</p> <p>18 Q. Okay. Did you -- why is that not</p> <p>19 true?</p> <p>20 A. Because I was asked to take a broader</p> <p>21 role as the head of global cyber partnerships.</p> <p>22 Q. And when you were asked to take the</p> <p>23 broader role, did you object to being removed as</p> <p>24 the CISO?</p> <p>25 A. I did not. Again, I wasn't removed as</p> <p style="text-align: center;">88</p>

Gregory Rattray
2/12/2025

<p>1 the CISO, so there was no objection to be made.</p> <p>2 Q. Well, you were no longer the CISO</p> <p>3 beginning in 2015, right?</p> <p>4 A. That's correct. I was asked to be the</p> <p>5 head of global cyber partnerships and work with</p> <p>6 the industry globally on matters of regulation and</p> <p>7 protection of the financial system.</p> <p>8 Q. And within the JPMorgan structure, a</p> <p>9 CISO is the -- a higher position than the head of</p> <p>10 global cyber partnerships, right?</p> <p>11 A. When I took the head of global cyber</p> <p>12 partnerships, I was a direct report to the chief</p> <p>13 administrative officer -- I'm sorry, the -- yeah,</p> <p>14 the chief administrative officer was actually a</p> <p>15 higher level of management than the chief</p> <p>16 information security officer.</p> <p>17 Q. Is that Paul Compton --</p> <p>18 A. Uh-huh.</p> <p>19 Q. -- that was the chief administrative</p> <p>20 officer?</p> <p>21 A. That's correct.</p> <p>22 Q. And before you reported to Paul</p> <p>23 Compton, who were you reporting to?</p> <p>24 A. Dana Deasy and Jim Cummings.</p> <p>25 Q. And, in fact, Rohan Amin became the</p> <p style="text-align: center;">89</p>	<p>1 THE WITNESS: No, I -- I mean, I</p> <p>2 recall discussions with the Secret Service. I</p> <p>3 wouldn't call them -- I wouldn't call them</p> <p>4 conflicts.</p> <p>5 BY MR. CARNEY:</p> <p>6 Q. Okay. Do you know Matthew Zames?</p> <p>7 A. I do know Matthew Zames.</p> <p>8 Q. Who is Matthew Zames?</p> <p>9 A. When I knew Matthew Zames, he was the</p> <p>10 chief operating officer for JPMorganChase.</p> <p>11 Q. Okay. And do you know Joseph</p> <p>12 Demarest?</p> <p>13 A. I do know Joseph Demarest. At the</p> <p>14 time, I believe he was the head of the -- he was</p> <p>15 the assistant director of the FBI for cyber.</p> <p>16 Q. And are you aware that Joseph Demarest</p> <p>17 with the FBI called Matthew Zames, the COO of</p> <p>18 JPMorgan, to discuss delays in access to the</p> <p>19 breached data that they wanted?</p> <p>20 A. I'm not at liberty to talk about the</p> <p>21 specifics of that incident.</p> <p>22 (Whereupon, Exhibit 3 is marked for</p> <p>23 identification.)</p> <p>24 BY MR. CARNEY:</p> <p>25 Q. All right. Dr. Rattray, I've handed</p> <p style="text-align: center;">91</p>
<p>1 CISO at JPMorgan in 2015, right?</p> <p>2 A. That's correct.</p> <p>3 Q. In 2014, when you were the CISO at</p> <p>4 JPMorgan, the company suffered one of the world's</p> <p>5 largest ever data breaches, right?</p> <p>6 A. It actually experienced the breach</p> <p>7 itself prior to my arrival at JPMorgan.</p> <p>8 Q. Okay. And is it fair to describe it</p> <p>9 that hackers exposed the names, addresses, phone</p> <p>10 numbers and email addresses of 83 million</p> <p>11 households and small business accounts?</p> <p>12 A. "Exposed" would probably be a</p> <p>13 mischaracterization.</p> <p>14 Q. Is it fair to say that when you -- so</p> <p>15 you were leading the response to the cybersecurity</p> <p>16 breach on behalf of JPMorgan; is that right?</p> <p>17 A. That's correct.</p> <p>18 Q. And is it fair to say that during the</p> <p>19 time you were leading that response, that you had</p> <p>20 conflicts with federal law enforcement agencies;</p> <p>21 is that right?</p> <p>22 A. That's not true.</p> <p>23 Q. Do you recall having conflicts with</p> <p>24 the Secret Service?</p> <p>25 MR. TURNER: Object to form.</p> <p style="text-align: center;">90</p>	<p>1 you what's been marked as Exhibit 3. And this is</p> <p>2 a June 30, 2015, article from Bloomberg.</p> <p>3 Have you ever seen this article</p> <p>4 before?</p> <p>5 A. Yes, I have.</p> <p>6 Q. And when was the first time you saw</p> <p>7 it?</p> <p>8 A. It was published in June 2015. I</p> <p>9 don't remember distinctly, but I probably saw it</p> <p>10 not long after its publication.</p> <p>11 Q. Okay. So if we can look at the first</p> <p>12 page of this article, and the article is entitled,</p> <p>13 "JPMorgan Reassigns Security Team Leader a Year</p> <p>14 After Data Breach."</p> <p>15 In that second paragraph, it says that</p> <p>16 "Greg Rattray, a former U.S. Air Force commander</p> <p>17 for information warfare and a cyber expert at the</p> <p>18 National Security Council under President</p> <p>19 George W. Bush no longer works as JPMorgan's chief</p> <p>20 information security officer, according to an</p> <p>21 internal memo sent June 11 and reviewed by</p> <p>22 Bloomberg News."</p> <p>23 Have you ever seen that memo?</p> <p>24 A. I actually don't know what memo this</p> <p>25 refers to.</p> <p style="text-align: center;">92</p>

Gregory Rattray
2/12/2025

<p>1 Q. Okay. On the next page, it says, 2 "Rohan Amin, a former cybersecurity executive at 3 Lockheed Martin Corp. who joined JPMorgan last 4 August, has replaced Rattray according to the 5 memo." 6 Was that an accurate statement? 7 A. Rohan took the job as the chief 8 information security officer. 9 Q. And then the next sentence says that, 10 "Rattray will oversee a few employees instead of 11 the hundreds he managed in JPMorgan's 12 cybersecurity unit." 13 Is that accurate? 14 A. Again, I think the hundreds figure is 15 low. You know, in terms of it numbered over a 16 thousand at that point. You know, I manage a 17 small team initially when I took over and built 18 the global cyber partnerships practice. 19 Q. All right. And then there's a bold 20 heading that says, "Limited access," and then in 21 the second paragraph, it says, "The Secret Service 22 grew so frustrated that it threatened to seize the 23 evidence, and Joseph Demarest, then assistant 24 director of the FBI's cyber division, called chief 25 operations officer Matthew Zames to discuss -- to</p> <p style="text-align: center;">93</p>	<p>1 break? 2 MR. TURNER: Sure. 3 THE VIDEOGRAPHER: The time right now 4 is 11:40 a.m. 5 We are off the record. 6 (Whereupon, a recess was taken at 7 11:41 a.m.) 8 THE VIDEOGRAPHER: The time right now 9 is 11:55 a.m. 10 We're back on the record. 11 BY MR. CARNEY: 12 Q. Okay. Dr. Rattray, I had just a 13 couple quick follow-ups about if we look at 14 Exhibit 2, your CV, page A-1. 15 A. Uh-huh. 16 Q. You see where it says, "Cofounder and 17 partner of Next Peak 2019 to the present"? 18 A. Yes. 19 Q. And did you hold both those positions 20 from 2019 to the present? 21 A. Both what positions? 22 Q. Cofounder and partner? 23 A. Well, yeah. I mean -- 24 Q. Okay. 25 A. -- I'm a cofounder and a partner --</p> <p style="text-align: center;">95</p>
<p>1 discuss the delays." 2 Do you have any reason to question the 3 accuracy of that? 4 A. I do. But I can't go into the 5 specifics of how we handled the incident. 6 Q. Okay. And then it says, "The 7 situation was resolved with a formal agreement to 8 share information." 9 Is that accurate? 10 A. Again, I can't go into the specifics 11 of our interactions between -- or not interactions 12 between JPMorganChase and the federal government. 13 Q. Okay. So just, sir, turning back to 14 your report, paragraph 8 -- after everything we 15 just discussed and looked at, do you stand by the 16 accuracy of that sentence from 2014 to 2019, "I 17 was chief information security officer and head of 18 global cyber partnerships at JPMorganChase where I 19 directed its cyber defense program and oversaw 20 more than a thousand personnel on a \$500 million 21 budget"? 22 A. Yes, I do. 23 Q. All right. 24 MR. CARNEY: Actually, I'm moving on 25 to a different subject. Do you want to take</p> <p style="text-align: center;">94</p>	<p>1 Q. Got it -- 2 A. -- yeah. 3 Q. -- okay. 4 And then similar with chief strategy 5 and risk officer, Andesite AI, 2023 to the 6 present, did you hold both of those positions from 7 2023 to the present? 8 A. Actually, no. I was originally just a 9 chief strategy officer, and then the team decided 10 to do sort of -- formally add "risk officer" to my 11 title. 12 Q. And when was that added? 13 A. Spring of 2024, I believe. 14 Q. All right. And then just with respect 15 to what we talked about on the next page, chief 16 information security officer and head of global 17 cyber partnerships, 2014 to 2019, sir, you'd agree 18 with me that in -- there's nowhere in your report 19 where it mentions that you stopped being the CISO 20 in 2015; is that right? 21 A. Yeah, it's not relevant to the -- my 22 task, you know, and assessment of the securities 23 statement. 24 Q. Okay. All right. Let's see. 25 Speaking of security statements, we talked a</p> <p style="text-align: center;">96</p>

Gregory Rattray
2/12/2025

<p>1 little bit about them earlier.</p> <p>2 But in terms of the public-facing</p> <p>3 security statements that we were talking about</p> <p>4 earlier, what is your understanding of the role</p> <p>5 that they play?</p> <p>6 A. You know, such -- you know, such</p> <p>7 public statements about security can play a very</p> <p>8 wide range of roles.</p> <p>9 Q. And what are those very wide range of</p> <p>10 roles?</p> <p>11 A. They can be, you know, just awareness</p> <p>12 that the company, you know, is -- you know,</p> <p>13 engaged -- you know, engaged in security. It can</p> <p>14 be, you know, as some of the things that were -- I</p> <p>15 was involved with, with JPMorgan statements, you</p> <p>16 know, that support industry efforts in</p> <p>17 cybersecurity.</p> <p>18 They can be -- you know, for the</p> <p>19 purpose that the SolarWinds statement was for,</p> <p>20 which is to sort of give people that are thinking</p> <p>21 about purchasing products some information about</p> <p>22 security practices of the company.</p> <p>23 I mean, the -- it was -- you know, we</p> <p>24 can continue with this, but there's probably</p> <p>25 very -- you know, very many purposes for a public</p> <p style="text-align: center;">97</p>	<p>1 And foundation.</p> <p>2 THE WITNESS: I don't know, you</p> <p>3 know -- I mean, how do I -- there were statements</p> <p>4 made. I'm not aware of statements that were made,</p> <p>5 you know, specifically to inform investors.</p> <p>6 BY MR. CARNEY:</p> <p>7 Q. So when you were making these public</p> <p>8 statements about cybersecurity at JPMorgan, who</p> <p>9 was the audience for those statements?</p> <p>10 MR. TURNER: Objection to form. And</p> <p>11 foundation.</p> <p>12 THE WITNESS: You know, again, in some</p> <p>13 cases, you know, we -- you know, we were working</p> <p>14 on, you know, things like the financial services</p> <p>15 sector cyber risk index that we worked together</p> <p>16 with NIST on. And there were, you know -- we</p> <p>17 declared our support for that -- for that effort.</p> <p>18 (Whereupon, Exhibit 4 is marked for</p> <p>19 identification.)</p> <p>20 BY MR. CARNEY:</p> <p>21 Q. I've handed you, Dr. Rattray, a</p> <p>22 document that's been marked as Exhibit 4, and it's</p> <p>23 a publication on Next Peak's website.</p> <p>24 A. Uh-huh.</p> <p>25 Q. It's called "Building a Focused</p> <p style="text-align: center;">99</p>
<p>1 statement about security.</p> <p>2 Q. Okay. And based on your experience,</p> <p>3 for instance, your experience at JPMorgan, do</p> <p>4 investors care about the cybersecurity practices</p> <p>5 of the firms in which they invest?</p> <p>6 MR. TURNER: Objection to form. And</p> <p>7 outside the scope of his assignment.</p> <p>8 THE WITNESS: Again, I don't -- you</p> <p>9 know -- you know, I don't know exactly what</p> <p>10 investors care about, right?</p> <p>11 BY MR. CARNEY:</p> <p>12 Q. Okay. So when you were at JPMorgan,</p> <p>13 for instance, was there -- and you mentioned</p> <p>14 JPMorgan put out public statements about its</p> <p>15 cybersecurity practices; is that right?</p> <p>16 A. At times, you know -- you know,</p> <p>17 especially related to joining industry</p> <p>18 associations and those sorts of things, we made</p> <p>19 statements we were involved with different sorts</p> <p>20 of security-related activities.</p> <p>21 Q. And were -- was one of the reasons</p> <p>22 that you were making those statements to inform</p> <p>23 investors about the company's cybersecurity</p> <p>24 practices?</p> <p>25 MR. TURNER: Objection to the form.</p> <p style="text-align: center;">98</p>	<p>1 Approach to Cyber Defense."</p> <p>2 Did you write this article?</p> <p>3 A. You know, similar to other discussions</p> <p>4 we've had, I think the team put it together.</p> <p>5 Yeah, so I don't have a recollection</p> <p>6 specifically about who -- who was the original</p> <p>7 drafter.</p> <p>8 Q. All right. If you would please, sir,</p> <p>9 turn to the third page of this article.</p> <p>10 A. Uh-huh.</p> <p>11 Q. Under the second paragraph under the</p> <p>12 heading "Why Next Peak Can Help," it -- it says,</p> <p>13 "Many companies, especially in the financial</p> <p>14 sector, often suffer drops in stock price</p> <p>15 following a cyberattack, however, JPMC stock</p> <p>16 actually rose slightly after the breach</p> <p>17 demonstrating how the steps the companies take</p> <p>18 during and after an incident can go a long way in</p> <p>19 reassuring stakeholders."</p> <p>20 Do you see that?</p> <p>21 A. I do see that.</p> <p>22 Q. And do you agree with that statement?</p> <p>23 A. I mean, I do agree with those</p> <p>24 statements. The data we cite is a Harvard</p> <p>25 Business Review -- Harvard Business Review</p> <p style="text-align: center;">100</p>

Gregory Rattray
2/12/2025

<p>1 article.</p> <p>2 Q. Do you agree -- let me break that up</p> <p>3 then.</p> <p>4 Do you agree that the steps that</p> <p>5 companies take during and after a cybersecurity</p> <p>6 incident can go a long way in reassuring</p> <p>7 stakeholders?</p> <p>8 A. Yes, I do.</p> <p>9 Q. And why was it relevant in your</p> <p>10 article that the stock price rose at JPMorgan</p> <p>11 following the attack?</p> <p>12 A. You know, the stock -- you know,</p> <p>13 stockholders are stakeholders in a company, right?</p> <p>14 And so this is an article meant to sort of</p> <p>15 portray, you know, concerns and how, again, as you</p> <p>16 just -- you know, you quoted why Next Peak can</p> <p>17 help.</p> <p>18 Q. And stockholders are investors in the</p> <p>19 company, right?</p> <p>20 A. Stockholders are equity owners in a</p> <p>21 company.</p> <p>22 Q. Okay. And so, in your view, as</p> <p>23 expressed in this article, stockholders are</p> <p>24 interested in companies' cybersecurity practices</p> <p>25 and how they respond to breaches, right?</p> <p style="text-align: center;">101</p>	<p>1 called to testify about materiality, that issue.</p> <p>2 Mr. Rattray has not offered any opinion as to</p> <p>3 materiality. That's not a subject of his report.</p> <p>4 So I'm just gonna object.</p> <p>5 This is outside the scope of his</p> <p>6 expert testimony.</p> <p>7 MR. CARNEY: Okay. And I think under</p> <p>8 the Federal Rules, you could have just used that</p> <p>9 last part, outside the scope.</p> <p>10 MR. TURNER: Well, I explained why it</p> <p>11 was outside the scope.</p> <p>12 MR. CARNEY: That's called a speaking</p> <p>13 objection --</p> <p>14 MR. TURNER: I understand.</p> <p>15 MR. CARNEY: -- which are improper.</p> <p>16 MR. TURNER: It's needed in this case.</p> <p>17 As it may --</p> <p>18 MR. CARNEY: There's no provision in</p> <p>19 the Federal Rules that call for speaking</p> <p>20 objections being needed, but okay.</p> <p>21 THE WITNESS: Are you going to repeat</p> <p>22 the question?</p> <p>23 BY MR. CARNEY:</p> <p>24 Q. Yeah. So the question was: The</p> <p>25 premise of your article that you wrote was that</p> <p style="text-align: center;">103</p>
<p>1 MR. TURNER: Object to form.</p> <p>2 THE WITNESS: You know, the article</p> <p>3 doesn't say, you know, stockholders are</p> <p>4 interested. So maybe we need to reframe the</p> <p>5 question or I need to rehear the question.</p> <p>6 BY MR. CARNEY:</p> <p>7 Q. Okay. All right.</p> <p>8 MR. TURNER: Are you asking him</p> <p>9 whether stockholders care about public statements</p> <p>10 like the securities statement, or are you asking</p> <p>11 about something else?</p> <p>12 MR. CARNEY: I'm asking him generally,</p> <p>13 stockholders care about a company's cybersecurity</p> <p>14 practices --</p> <p>15 BY MR. CARNEY:</p> <p>16 Q. -- right? According to your</p> <p>17 article --</p> <p>18 MR. TURNER: I'm just going to</p> <p>19 object --</p> <p>20 (Simultaneous unreportable crosstalk</p> <p>21 occurs among parties.)</p> <p>22 (Stenographer requests one speaker at a</p> <p>23 time.)</p> <p>24 MR. TURNER: I'm going to object.</p> <p>25 You called two witnesses who you</p> <p style="text-align: center;">102</p>	<p>1 shareholders could be reassured if a company went</p> <p>2 out and showed how they were dealing with a cyber</p> <p>3 breach, right?</p> <p>4 A. The premise was -- of the article was</p> <p>5 that we could help build that focused approach to</p> <p>6 cyber -- that's the premise of the article.</p> <p>7 Q. All right. Sir, I want to ask you</p> <p>8 about your opinions related to the NIST</p> <p>9 Cybersecurity Framework.</p> <p>10 A. Uh-huh.</p> <p>11 Q. And if you look -- I think if you turn</p> <p>12 to paragraph 31.</p> <p>13 A. Of my expert report?</p> <p>14 Q. Of your expert report, Exhibit 1, it</p> <p>15 should be.</p> <p>16 A. Uh-huh.</p> <p>17 Q. And you say that the NIST</p> <p>18 Cybersecurity Framework was first established in</p> <p>19 2014, right?</p> <p>20 A. Again, I made a mistake. I looked at</p> <p>21 page 31, not paragraph 31.</p> <p>22 Q. Yeah, page 10.</p> <p>23 A. Yes.</p> <p>24 Q. Okay.</p> <p>25 A. And I'm on page -- paragraph 31.</p> <p style="text-align: center;">104</p>

Gregory Rattray
2/12/2025

<p>1 Q. Okay. And you state that the NIST 2 Cybersecurity Framework was first established in 3 2014, right? 4 A. That's correct. 5 Q. And that was during the time that you 6 were at JPMorgan, right? 7 A. Yes, that's correct. Again, I don't 8 know if it was early 2014 and if I had arrived at 9 JPMorgan, but I arrived at JPMorgan in the summer 10 of 2014. 11 Q. Did JPMorgan follow the NIST 12 Cybersecurity Framework when you were there? 13 A. JPMorgan -- again, I can't -- I'm 14 going to sort of be limited to how detailed I can 15 go. 16 JPMorgan led an industrywide effort 17 to, you know, create an industry-driven framework 18 called the cyber risk index based on the NIST 19 Cybersecurity Framework. 20 What was... 21 You know -- you know, so, yeah, you 22 know, that was clearly, you know, something that 23 actually I led as the head of global cyber 24 partnerships for the firm and for the industry. 25 Q. So the cyber risk index was based on</p> <p style="text-align: center;">105</p>	<p>1 team," who was on the leadership team? 2 A. The CISO, the chief compliance officer 3 of the firm, the implementation people for 4 regulatory compliance within the cybersecurity 5 team. 6 Q. So who had responsibility at JPMorgan 7 for ensuring that this framework that you just 8 discussed was followed? 9 A. Again, there was no -- there was -- 10 there was no requirement for compliance with the 11 framework. 12 Q. Okay. Putting aside a requirement for 13 compliance, was JPMorgan trying to follow the 14 Cyber Risk Institute framework that you discussed? 15 A. Again, during -- 16 MR. TURNER: Object to form. 17 THE WITNESS: Right. 18 Again, that developed over a period of 19 years. JPMorgan, you know, broadly utilized the 20 cyber -- the cybersecurity -- the NIST 21 Cybersecurity Framework, and then, you know, that 22 informed its work on the -- what became the Cyber 23 Risk Institute's framework, which is deeply NIST 24 CSF based. 25 Just like, you know, NIST called for</p> <p style="text-align: center;">107</p>
<p>1 the NIST Cybersecurity Framework? 2 A. Yes. Or it's actually cyber risk 3 institutes, you know, cyber framework. I'm sorry. 4 I shouldn't have said "index." I should have said 5 "institute." 6 Q. Okay. And you say it was based on the 7 NIST Cybersecurity Framework. 8 What does that mean? 9 A. We were in a situation where the 10 industry was getting from various regulators 11 different -- different regulatory requirements. 12 And as an industry, there was an effort to work to 13 establish a framework that was NIST aligned. 14 But specific to cybersecurity, NIST 15 had supported such efforts with other industries 16 and supported the effort that we undertook, you 17 know, in the financial services industry. 18 Q. And did you have any responsibility 19 for ensuring that JPMorgan followed that framework 20 that you just discussed? 21 A. I was in constant discussions with the 22 leadership team about the nature of the framework 23 that was being derived and how it would enable 24 our, you know, cyber program and compliance. 25 Q. Okay. When you say "the leadership</p> <p style="text-align: center;">106</p>	<p>1 as general guidance for, you know, firms to 2 understand their state of practice and, you know, 3 guide -- guide efforts for the NIST Cybersecurity 4 Framework is not something to be followed, per se. 5 It's guidance to enable cybersecurity program. 6 BY MR. CARNEY: 7 Q. And so I guess my question then is 8 that JPMorgan -- whatever they were doing with the 9 NIST Cybersecurity Framework, using it as 10 guidance -- 11 A. Uh-huh. 12 Q. -- who had responsibility for ensuring 13 that they were using the NIST Cybersecurity 14 Framework as guidance? 15 MR. TURNER: Object to form. 16 THE WITNESS: Yeah, I mean, the -- 17 there wasn't a singular person. It was a 18 decision, you know, by a number of people, and 19 basically the people that I've described, probably 20 others involved including the general counsel, 21 about, you know, what sort of framework should 22 guide the program in a -- in a heavily regulated 23 environment. 24 So, you know, there was not a singular 25 individual responsible.</p> <p style="text-align: center;">108</p>

Gregory Rattray
2/12/2025

<p>1 BY MR. CARNEY: 2 Q. And you -- you said there were a group 3 of individuals. 4 Were you one of the individuals? 5 A. Yes -- 6 Q. Okay. 7 A. -- I mean, okay, yes. 8 Q. What is the basis for your statement 9 that the NIST Cybersecurity Framework is not 10 something to be followed? 11 A. You know, I just want to use the quote 12 that I provided in -- in my report, which 13 basically is NIST language around, you know, this 14 is a voluntary -- oh, quoting from the framework. 15 "The framework is voluntary and there 16 is no right or wrong way to do it." 17 Q. What page are you on? 18 A. I'm on page 13, the end of 19 paragraph 36. 20 Q. Sir, I'm going to ask you -- let me 21 back up for a second. 22 Did JPMorgan ever perform assessments 23 to see whether it was compliant with the NIST 24 Cybersecurity Framework? 25 MR. TURNER: Objection to form.</p> <p style="text-align: center;">109</p>	<p>1 Q. Okay. Putting aside JPMorgan, do you 2 personally have any experience assessing whether a 3 company was compliant with the NIST Cybersecurity 4 Framework? 5 MR. TURNER: Object to form. 6 "Compliant." 7 THE WITNESS: Right. Again, as just 8 described, the framework is voluntary, and there's 9 no right or wrong way to use it. It explicitly 10 doesn't call for compliance. It calls for, you 11 know, voluntarily use in self-evaluation. 12 To the point of the question, I have 13 numerous experiences helping companies assess 14 themselves under the NIST Cybersecurity Framework. 15 BY MR. CARNEY: 16 Q. And what was your role in those 17 assessments? 18 A. You know, everything from interviewing 19 people about the presence of controls and certain 20 control areas up to working with the leadership 21 team about the -- you know, the outputs of the 22 evaluation and the scoring and even at times in 23 some of the cases helping brief -- brief the 24 assessment company leadership. 25 Q. Have you ever personally assessed</p> <p style="text-align: center;">111</p>
<p>1 "Compliant." 2 THE WITNESS: Yeah, I'm not probably 3 at liberty to talk about exactly how JPMorgan 4 self-assessed itself. 5 BY MR. CARNEY: 6 Q. Without getting into the details, did 7 they assess themselves under the NIST 8 Cybersecurity Framework? 9 A. Again, that's a detail, in my 10 estimation. I mean -- 11 (Zoom participant interrupts.) 12 THE STENOGRAPHER: Excuse me. Can the 13 people on Zoom please mute themselves? 14 Sorry. If you could repeat your 15 answer. 16 THE WITNESS: Can we repeat that 17 question? 18 BY MR. CARNEY: 19 Q. Sure. 20 Without getting into details, did 21 JPMorgan assess themselves under the NIST 22 Cybersecurity Framework? 23 A. Again, I think, you know, the details 24 of JPMorgan's self-assessment probably goes beyond 25 what I, you know, am obligated not to do.</p> <p style="text-align: center;">110</p>	<p>1 maturity levels under the NIST Cybersecurity 2 Framework? 3 A. Yes. 4 Q. And what was your role in assessing 5 maturity levels? 6 A. As I just described, everything for 7 certain control areas down to looking at the 8 presence of policy, talking with leaders, looking 9 for specific evidence that control structures were 10 in -- and implementation or active and also 11 looking at other assessments like audit 12 assessments about the presence of the practice. 13 Q. Okay. Doctor, if you could look at 14 page 62 of your report, please. 15 A. Page 62, correct? 16 Q. Yes, sir. And it's paragraph 112, 17 which starts on the prior page. 18 A. Uh-huh. 19 Q. And do you see within the body of the 20 report sort of towards the end of page 62, you 21 quote the General Motors Financial Company 10-K 22 for fiscal year 2023? 23 A. I do see that. 24 Q. And it states, "We design and assess 25 our program based on the National Institutes of</p> <p style="text-align: center;">112</p>

Standards and Technology Cybersecurity Framework," and then in parentheses, "NIST CSF."

"This does not imply that you meet any technical standards, specifications or requirements, but rather that we use the NIST CSF as a guide to help us identify, assess and manage cybersecurity risks relevant to our business."

Did I read that correctly?

A. Yes.

Q. All right. And you have in footnote in -- in Footnote 145 to that paragraph --

A. Uh-huh.

Q. -- you quote the 10-Ks of Digital Realty Trust and SkyWest; is that right?

A. I just want to make sure that we get the right companies. I see SkyWest. I see GMFC. I'm just -- I'm just looking for the digital real -- there it is. Yep, I see all three companies in the footnote.

Q. Great. And Digital Realty Trust Inc. and SkyWest Inc., they have similar language to the GMFC 10-K statement regarding the NIST framework, right?

A. Yes.

Q. And specifically each of them include

113

the sentence "This does not imply that we meet any particular technical standards, specifications or requirements but rather that we use the NIST CSF as a guide to help us identify, assess and manage cybersecurity risks relevant to our business," right?

A. Yeah, I would agree that all three companies have similar language in these 10-K declarations.

Q. And what is your understanding of the purpose of that sentence in those three 10-Ks?

A. I couldn't speak to the -- you know, why any given company decided to put that sentence in, because the NIST Cybersecurity Framework lays out itself, you know, in detail that that is the case.

I mean, this says NIST framework is -- you know, does not imply that you should meet any particular technical standard, and it's voluntary to be used as a company sees fit.

Q. Okay. And let's just use the General Motors Financial Company as one example.

A. Uh-huh.

Q. Would you agree that without that sentence, that the meaning of the paragraph is

114

different?

A. No.

Q. So you think that sentence adds nothing, in your opinion?

A. As I just stated, because NIST basically makes itself -- makes the statements that, you know, are outlined here, we could look at specifics from the framework.

But NIST itself says in publishing the framework that it's not, you know -- does not require or imply that a company does anything specific in terms of technical standards and specifications. And it's meant to be used as a guide.

You know, I find the sentence repetitive and not -- you know, not additive.

Q. Okay. So in the first sentence, it says, "We designed and assess our program based on the National Institutes of Standards and Technologies Cybersecurity Framework, right?"

A. Uh-huh. Yes.

Q. And you don't think that that second sentence adds anything to clarify what they mean by that first sentence?

A. I mean, that's up to the people making

115

this statement about whether they -- you know, they believe -- I believe it's repetitive, because, you know, the NIST Cybersecurity Framework itself tells you the things that are in that sentence.

Q. So one would have to go look at the NIST Cybersecurity Framework itself to understand the first sentence without that second sentence, right?

A. Yeah, I'm just trying to process what the question is.

MR. TURNER: Object to form.

Go ahead.

BY MR. CARNEY:

Q. Yeah, the question is that without that second sentence or some independent understanding of what NIST itself has said about the cybersecurity framework, that first sentence would mean something different, right?

A. No. It would mean exactly what it said, right? Like, we design and assess our program based on the NIST -- the National Institute of Standards in Technology's Cybersecurity Framework. I don't understand how -- I just don't understand how dropping the second

116

Gregory Rattray
2/12/2025

<p>1 sentence changes the meaning of the first 2 sentence.</p> <p>3 Q. Okay. All right. And I'll represent 4 to you that according to the NIST website, the 5 cybersecurity framework is a set of best 6 practices, standards and recommendations.</p> <p>7 Do you have any reason to disagree 8 with that?</p> <p>9 A. Well, I, yeah, need to see where in 10 the -- you know, the NIST website, which is 11 probably voluminous, because, you know, as stated 12 in my, you know, expert report, it basically says 13 that that -- you know, it's voluntary. And, you 14 know, is to be used as see fit. So it's not 15 directive.</p> <p>16 Again, we probably have to compare the 17 language you just said to, you know, other 18 language within the NIST cybersecurity framework's 19 website.</p> <p>20 Q. Okay. And you just said the website 21 is voluminous; is that right?</p> <p>22 A. Well, you know, as I said, I think 23 it's probably voluminous, because, you know, 24 having been on NIST websites, you know, they -- 25 they sort of link to a lot of things, right?</p> <p style="text-align: center;">117</p>	<p>1 (Whereupon, Exhibit 5 is marked for 2 identification.)</p> <p>3 BY MR. CARNEY:</p> <p>4 Q. All right. Dr. Rattray, I've handed 5 you what's been marked as Exhibit 5. And I'll 6 represent to you that this is a copy of 7 SolarWinds's security statement that the parties 8 have stipulated is basically the way it appeared 9 during the relevant period.</p> <p>10 Have you seen this document before 11 or --</p> <p>12 A. Yes, I have --</p> <p>13 Q. -- some version of it?</p> <p>14 A. -- yep.</p> <p>15 Q. Sir, if you could turn to -- on the 16 first page where it says -- under organizational 17 security, it says, "SolarWinds follows the NIST 18 Cybersecurity Framework with layered security 19 controls to help identify, prevent, detect and 20 respond to security incidents."</p> <p>21 You see that, right?</p> <p>22 A. I do.</p> <p>23 Q. And you would agree with me that that 24 statement does not have a caveat like the ones 25 that we looked at for General Motors, for Digital</p> <p style="text-align: center;">119</p>
<p>1 So I don't know what the front page of 2 the NIST Cybersecurity Framework website looks 3 like at the moment. I don't know what it looked 4 like specifically during the relevant period.</p> <p>5 I do know that, you know, it clearly 6 stated, you know, that the framework itself is 7 voluntary and calls on the companies to, you know, 8 use it as they see fit.</p> <p>9 Q. And is that -- is somewhere on the 10 voluminous website that it states that it's a 11 voluntary standard?</p> <p>12 A. As I said, I don't know for sure if 13 it's voluminous. I said I expect that it is 14 having been on standard-setting organizations' 15 websites many times, and often they are -- they 16 have a lot of links and, therefore, there's a lot 17 of information on it.</p> <p>18 I don't know specifically, you know, 19 what instance of the website at what time we're 20 discussing here.</p> <p>21 MR. TURNER: I'll note for the record, 22 Mr. Graff is quoting a document that is found on 23 the NIST website as reflected in his report.</p> <p>24 MR. CARNEY: All right.</p> <p>25 ///</p> <p style="text-align: center;">118</p>	<p>1 Realty Trust or for SkyWest; is that right?</p> <p>2 A. You know, we have the security 3 statement in front of us. It doesn't have a 4 caveat in -- for the -- as I mentioned previously, 5 the caveats were repetitive.</p> <p>6 Q. Okay. And if we look at -- on page 62 7 that we were just looking at in Exhibit 1 8 underneath the quote from GMFC --</p> <p>9 A. Yes.</p> <p>10 Q. -- you write, "I understand the 11 representation about the NIST CSF in the 12 securities statement in the same way" --</p> <p>13 A. Uh-huh.</p> <p>14 Q. -- "not a statement that SolarWinds 15 met any particular technical standards, but rather 16 as a statement about its cybersecurity governance, 17 i.e., a statement that it regularly assessed its 18 cybersecurity posture and used the NIST CSF as a 19 guide in doing so."</p> <p>20 Do you see that?</p> <p>21 A. I do see that.</p> <p>22 Q. So is it -- is it fair to say that 23 even though the securities statement doesn't 24 contain the caveat that the other companies 25 included, you are interpreting it as if it did?</p> <p style="text-align: center;">120</p>

Gregory Rattray
2/12/2025

<p>1 A. I'm just trying to understand the 2 question. 3 You know, I don't need to -- I guess 4 the -- my thinking is revolving around the notion 5 of the word "interpret," right? 6 The NIST Cybersecurity Framework 7 itself says it's, you know, not meant to be a set 8 of technical standards, and it's supposed to be a 9 guide to cybersecurity governance. 10 So there's really, you know, no need 11 for interpretation, because the framework itself 12 calls for this. 13 Q. Would you expect that, let's say a 14 layperson, someone who is not an expert in 15 cybersecurity, would read SolarWinds's security 16 statement and also read in that limitation or 17 caveat into it? 18 A. I believe that the security statement 19 is not designed to be read by laypersons. The 20 security statement is meant -- you know, was built 21 and is designed in order to, you know, provide 22 information to potential users of SolarWinds's 23 products about its security practices. 24 And that to me means the people 25 looking at this have some understanding of</p> <p style="text-align: center;">121</p>	<p>1 want to be sure, because I'm reading the first 2 sentence of that paragraph 40, and I don't see the 3 word "accurate" in it. I just want to make sure 4 I'm on the -- 5 (Simultaneous unreportable crosstalk 6 occurs among parties.) 7 (Stenographer requests one speaker at a 8 time.) 9 THE WITNESS: Yeah, so I see the 10 heading (c) above paragraph 40 saying the 11 securities statement's representation about 12 role-based were accurate. 13 Yeah, just to clarify, because I went 14 right to the paragraph 40. 15 BY MR. CARNEY: 16 Q. Understand. Thank you. 17 Sir, if you could turn a couple pages 18 forward, I just wanted to sort of show you what 19 section we were in, but paragraph 44 -- 20 A. Uh-huh. 21 Q. -- you state, "I have reviewed samples 22 from over a thousand SARFs" -- and that's S-A-R-F, 23 and then plural, SARFs -- 24 A. Uh-huh. 25 Q. -- "I have received that were filled</p> <p style="text-align: center;">123</p>
<p>1 cybersecurity and cybersecurity governance. 2 MR. TURNER: Chris, just want to flag, 3 the next 15 minutes or so would be good to break 4 for lunch, whenever is good. 5 MR. CARNEY: Yeah, so why don't we 6 break in 15 then? Is that cool? 7 MR. TURNER: In 15 minutes? 8 MR. CARNEY: Yeah. 9 MR. TURNER: Sure. 10 BY MR. CARNEY: 11 Q. All right. I'm going to shift topics 12 now, sir, to ask you about role-based access 13 controls. So if you look at the page 40 of 14 Exhibit 1 -- I'm sorry. Apologies. I just did 15 that myself. 16 A. Oh. 17 Q. If you look at page 15, 18 paragraph 40 -- 19 A. Paragraph 40 -- 20 Q. -- and there's a heading that says 21 "The Securities Statement Representations About 22 Role-Based Access Controls Were Accurate." 23 And I want to direct your attention, 24 sir, to a couple pages forward on page -- 25 A. Excuse me. Just what you -- I just</p> <p style="text-align: center;">122</p>	<p>1 out for newly hired employees during the relevant 2 period, evidencing they were completed as a 3 regular practice." 4 So I want to ask you -- and there's a 5 Footnote -- 6 A. Uh-huh. 7 Q. -- 28, and by my count, there are 8 eight examples listed there, eight samples. 9 First of all, who selected these 10 samples for you? 11 A. As we've discussed, when I asked for 12 evidence of, like, the SARFs, that just some 13 access request forms -- or, you know, evidence of 14 the presence of practice around role-based access 15 control, that I called them data tranches. 16 The tranche was created for me, and I 17 received it from Latham. I made the selection of 18 the cited examples in the report. 19 Q. Okay. And how did you go about 20 choosing those eight samples? 21 A. I reviewed, you know, usually 50 to 22 70 documents in these tranches and, you know, 23 decided, you know, looked at if the proper number 24 is 8 -- I think -- yeah, I'll just assume it's 8, 25 you know, 8 or 10 in many cases of these large</p> <p style="text-align: center;">124</p>

1 evidence sets that, you know, sort of illustrative
2 examples from the 50 to 70 that I reviewed.

3 **Q.** And putting aside the -- so aside from
4 the 50 to 70 that you reviewed, how do you know
5 what were in the other, let's say, thousand or so
6 SARFs that you didn't look at?

7 **A.** You know, similar to, you know, any
8 sort of large data set practice where you're
9 trying to look at -- you know, 50 to 70 is
10 actually a large number to look at in the conduct
11 of an assessment or, you know, of a security
12 control in terms of, you know, getting a sense of
13 whether, you know, this implementation was
14 actually, you know, well -- well conducted in
15 practice.

16 So I felt like 50 to 70 was more than
17 enough to indicate that the SARF process was in
18 place and executed fully.

19 **Q.** Why was 50 to 70 more than enough?

20 **A.** Because that's a pretty -- like, there
21 was very little deviation in those samples. They
22 showed the right sort of process, execution. And
23 they're actually very -- sort of very deep in
24 that -- in that sense.

25 So, again, having done many, many

125

1 based on the content of the SARF documents
2 themselves?

3 **MR. TURNER:** Objection to form.

4 And objection -- just --

5 **THE WITNESS:** Go ahead. Yep.

6 **MR. TURNER:** Yeah, objection to form.

7 And to the characterization of the report.

8 **THE WITNESS:** You know, it was
9 basically the second, though, of course -- you
10 know, the fact that they existed was part of the
11 evaluation that their -- you know, a policy and
12 procedure for role-based access was in place.

13 But, you know, examining that, you
14 know, the reports themselves, you know, my -- my
15 judgment, you know, based upon seeing how this
16 access control is provisioned, you know, and
17 managed in other environments, this seemed a very
18 thorough, sort of above and beyond process for
19 doing so.

20 **BY MR. CARNEY:**

21 **Q.** All right. So you said basically it
22 was the second.

23 So you were relying on the content of
24 the SARFs themselves?

25 **MR. TURNER:** Objection --

127

1 assessments, that level of sort of evidence
2 examination, you know, is more than sufficient in
3 my estimation to, sort of, you know, validate
4 that -- this element of the role-based access
5 processes was well executed.

6 **Q.** Now, to pick the 50 to 70, did you use
7 any kind of sampling methodology?

8 **A.** I wanted to make sure I looked across
9 the relevant period, that I looked across
10 different business units, different geographic
11 locations of the company.

12 **Q.** Okay. And so what led you, if you
13 did, to believe that the eight samples that you
14 cite in Footnote 28 are representative of the
15 larger body of SARFs at SolarWinds?

16 **A.** I chose them based on those same
17 criteria that I just mentioned across that
18 relevant period; business units, to the extent to
19 which I could, and then geographic regions.

20 **Q.** The exclusion that you've reached -- I
21 think you mentioned a little while ago that this
22 element of the role-based access processes was
23 well executed.

24 Was that based on the mere existence
25 of the SARF, or did you reach your conclusions

126

1 **THE WITNESS:** No, I said it was --

2 **MR. TURNER:** -- vague.

3 **THE WITNESS:** Yeah, go ahead.

4 **MR. TURNER:** Object to form.

5 Go ahead.

6 **THE WITNESS:** No. I said it was both,
7 right? I mean, I literally said, you know, that
8 the -- you know, the first is important to show
9 that they had a -- you know, general process, you
10 know, for doing this which, you know, I have no
11 reason to doubt was well executed, you know,
12 across the company.

13 And then I looked at the specific
14 content to make sure that the execution itself was
15 at -- you know, a strong level.

16 **BY MR. CARNEY:**

17 **Q.** And that's -- when you looked at the
18 specific content, did you only look at the
19 specific content for these eight samples?

20 **A.** No. I looked at the specific content
21 for the 50 to 70 samples.

22 **Q.** And so what would a SARF document have
23 to include for you to conclude that SolarWinds's
24 access controls were inconsistent with the
25 assertions in the securities statement?

128

Gregory Rattray
2/12/2025

<p>1 A. I think I want to work a little bit on 2 just what the question is. 3 Q. Sure. 4 A. I mean, you know, like, I'm trying to 5 figure out how you could even find evidence in 6 something of inconsistency -- right? -- like, you 7 know, on a given form. 8 You know, so could you just repeat the 9 question one time? 10 Q. Sure, sure. 11 I'm trying to understand, you looked 12 at these SARF documents -- 13 A. Right. 14 Q. -- and concluded that they were 15 consistent with what SolarWinds said in its 16 public- -- 17 A. Right. 18 Q. -- facing security statement -- 19 A. Right. 20 Q. -- right? 21 A. Yeah. 22 Q. And I'm wondering what would you have 23 had to have seen in the SARFs, hypothetically, to 24 have reached the opposite conclusion that 25 SolarWinds was not doing what it said in the</p> <p style="text-align: center;">129</p>	<p>1 inconsistency anywhere. 2 BY MR. CARNEY: 3 Q. All right. And if you guys can 4 indulge me for a couple more minutes, I have one 5 exhibit related to this, and then we'll break. 6 (Whereupon, Exhibit 6 is marked for 7 identification.) 8 BY MR. CARNEY: 9 Q. All right, Doctor. And take as much 10 time as you need to look at it, but I've handed 11 you what's been marked as Exhibit 6. 12 And I'm tell you what I did is I took 13 the eight SARFs you cite as samples in 14 Footnote 28, and I put them together as one 15 exhibit. I tried to do it in Bates number order. 16 But if we can look at the first page, 17 the first SARF -- 18 A. Uh-huh. 19 Q. -- and it's Bates ending in -- so it's 20 SW-SEC-SDNY- -- 21 A. Uh-huh. 22 Q. -- 55459, just, for the record. 23 A. Uh-huh. 24 Q. You see that an employee named Zouhair 25 Khadija is being requested -- is having access</p> <p style="text-align: center;">131</p>
<p>1 security statement? 2 MR. TURNER: Object to form. 3 THE WITNESS: You know, again, it 4 would have -- well, first, it would have been a 5 matter of degree of execution, because they had a 6 policy. They, you know, clearly had process -- 7 the SARF process in place. 8 And it was -- you know, again, lots of 9 data showing its implication. And actually 10 outside auditors had also reviewed the same data 11 and said that this was -- you know, that they were 12 implementing this process and made no findings. 13 You know, in -- you know, my case, if 14 I had sort of consistently seen that the -- you 15 know, the name field was not filled in, that -- 16 you know, at some large number of the sample -- 17 the 50 to 70 I looked at were missing the name 18 field, that would have been -- that would have 19 been a -- you know, a red flag. 20 In which case, I probably would have 21 looked to -- you know, talked to the people like I 22 did in those other couple cases we've talked about 23 related to evidence samples about how they used 24 the data. 25 But, like, I did not see that level of</p> <p style="text-align: center;">130</p>	<p>1 requested, right? 2 A. Yes. 3 MR. TURNER: Object to form. 4 It's labeled "change in role/access." 5 THE WITNESS: Oh, okay. 6 BY MR. CARNEY: 7 Q. All right. 8 MR. TURNER: I'm just clarifying that 9 they're not getting access for the first time, if 10 that's what you -- request access. 11 THE WITNESS: All right. 12 MR. CARNEY: Thanks for the 13 clarification. 14 BY MR. CARNEY: 15 Q. What access was this employee being 16 given? 17 A. As was just mentioned, this is a 18 change in -- so this, again, is not initial 19 provisioning of access. 20 This is the portion of the process 21 where SolarWinds also -- you know, if they -- a 22 person changed roles, you know, the process looked 23 through to redefine, you know -- that the 24 role-based access based on the new role. 25 You know, you see on the reverse of</p> <p style="text-align: center;">132</p>

Gregory Rattray
2/12/2025

<p>1 the form -- right? -- you know, detail about for 2 certain roles, you know, what were the standard 3 accesses for those roles. 4 So, you know, and then we see system 5 and area under the, you know, "Outlook 6 Distribution Lists." So this -- this entire 7 process, you know, would have re-rolled his access 8 in, you know, according to a standardized process 9 that SolarWinds had for different -- different 10 roles within the company. 11 Q. Okay. And to sort of counsel's 12 objection, clarification, that this was a change 13 in the access that this individual had -- 14 A. Uh-huh. 15 Q. -- what was it being changed from? 16 What was it before? 17 MR. TURNER: Objection. Foundation. 18 THE WITNESS: Again, you know, in this 19 case, it's pretty clear from what's on the form 20 itself that he was going to a new location in 21 Austin and -- you know, a new division, finance. 22 Yeah, so, I mean -- you know. 23 But, again -- you know, I did not -- 24 you know, analyze every field of every of the 50 25 to 70 forms nor the eight that are presented.</p> <p style="text-align: center;">133</p>	<p>1 was given actually match up with what's on the 2 SARF? 3 A. What's the question? What... 4 Q. Yeah, so I'm just trying to understand 5 how we know that this person that accessed this 6 form says they should be given is what they were 7 given. That's all I'm trying to understand. 8 A. Yeah, I mean, the securities statement 9 calls for the presence of role-based access. 10 There's a process in this form, you know, in -- 11 you know, and the testimony indicates that this 12 form maps directly to accesses that the IT team 13 would implement for different job descriptions 14 like Austin and finance. 15 You know, the fact that this process 16 is -- you know, robust and detailed, even years 17 after, we can find artifacts about how this was 18 occurred -- makes me highly confident that what 19 they said they were doing, they did. 20 MR. TURNER: Why don't we break here. 21 You've been going 20 minutes. 22 MR. CARNEY: Just one more question. 23 MR. TURNER: One more. 24 THE WITNESS: Uh-huh. 25 ///</p> <p style="text-align: center;">135</p>
<p>1 BY MR. CARNEY: 2 Q. Can you tell from this form what 3 access rights this employee was given as opposed 4 to what he was supposed to be given? 5 MR. TURNER: Objection to form. 6 THE WITNESS: Yeah, you know, this 7 form implements a process that was also described 8 in depositions by the technology leadership that, 9 you know, was meant to, you know, provide a lot of 10 control over what access is. 11 This is a process that there's a lot 12 of instances on, so they -- they move to, you 13 know, increasing levels of automation even during 14 the period -- you know, the relevant period in the 15 execution of the SARF process. 16 So I think, you know, in terms of this 17 form in which of the distro- -- like, the -- the 18 role itself has accesses -- you can map to 19 accesses on the back form. 20 The form would then go to the 21 technology team for implementation. So the form 22 wasn't the only part of the process, right? 23 BY MR. CARNEY: 24 Q. Okay. So what would you need to look 25 at to see that the access rights that the employee</p> <p style="text-align: center;">134</p>	<p>1 BY MR. CARNEY: 2 Q. And I'm just asking from, like, a 3 technical standpoint. Zouhair Khadija, if I 4 wanted to know that this person got the accesses 5 that this form indicates they were gonna get back 6 in 2017, what would I look at to make sure it was 7 done correctly? 8 A. Yeah, I, you know, is this a 9 hypothetical -- 10 Q. No. This is about this person here. 11 A. Okay. You know, I'm just trying to -- 12 like, the form tells you which of the systems are 13 listed in the back for role -- are you asking 14 whether you're actually gonna go to the person's 15 computer and, like, assess, you know, computer by 16 computer whether that person actually can only 17 get -- you know, has access to the things that are 18 listed in the process, you know -- they can go -- 19 you could go to the person's computer at the point 20 in time and determine whether the accesses -- you 21 know, sort of outlined by the form. 22 But the point of the securities 23 statement and, you know, the assessment I did was 24 to basically, you know, look at the fact that 25 these things were in place. And this is the</p> <p style="text-align: center;">136</p>

Gregory Rattray
2/12/2025

<p>1 typical way the companies do this.</p> <p>2 And the executives of the companies</p> <p>3 said they did it, and outside auditors also</p> <p>4 validated that they had proper role-based access</p> <p>5 control.</p> <p>6 Q. Okay. Last question before we break.</p> <p>7 What I'm understanding is there's no</p> <p>8 way you've described an artifact that I can look</p> <p>9 at now and say -- see that Zouhair Khadija got the</p> <p>10 specific access controls that are listed in this</p> <p>11 document; is that fair to say?</p> <p>12 MR. TURNER: Objection to form. And</p> <p>13 foundation.</p> <p>14 THE WITNESS: You know, we -- I mean,</p> <p>15 there could be discovery probably about -- you</p> <p>16 know, forensic images of his computer. I don't</p> <p>17 know if those exist or not.</p> <p>18 So I'm hesitant to say there's no</p> <p>19 artifact you could go look for. But it's not</p> <p>20 necessary in the nature of the assessment I did,</p> <p>21 because there's deep evidence that there -- you</p> <p>22 know, that this is an implementation of a practice</p> <p>23 of role-based access control.</p> <p>24 You know, they clearly had process.</p> <p>25 They were doing the process. The management</p> <p style="text-align: center;">137</p>	<p>1 SARFs from Footnote 28 in your report.</p> <p>2 A. Yes.</p> <p>3 Q. I just want -- one more question about</p> <p>4 these.</p> <p>5 You understand that there are tickets</p> <p>6 associated with SARFs; is that right?</p> <p>7 A. I understand that, you know, SARFs</p> <p>8 generate user access requests or, you know,</p> <p>9 tickets.</p> <p>10 Q. Okay. And with respect to the eight</p> <p>11 samples that are in Exhibit 6, did you examine the</p> <p>12 tickets associated with these SARFs?</p> <p>13 A. You know, I -- I examined a number of</p> <p>14 the tickets. I actually don't remember if I</p> <p>15 met -- I don't remember mapping those tickets to</p> <p>16 these SARFs.</p> <p>17 Q. Okay. So you're not sure one way or</p> <p>18 the other whether you looked at the tickets</p> <p>19 associated with these SARFs?</p> <p>20 A. Yeah. That was, again, sort of below</p> <p>21 the level of analysis that I thought was</p> <p>22 appropriate -- given that, you know, the fact that</p> <p>23 both that SARF process and that user access</p> <p>24 request, you know, tickets really demonstrated</p> <p>25 what the security statement called for.</p> <p style="text-align: center;">139</p>
<p>1 testified that that process was in place and being</p> <p>2 executed. Outside auditors looked at the process</p> <p>3 and validated that it was in place.</p> <p>4 So there was no need to go deeper than</p> <p>5 this.</p> <p>6 BY MR. CARNEY:</p> <p>7 Q. All right. Thanks.</p> <p>8 THE VIDEOGRAPHER: The time right now</p> <p>9 is 12:52 p.m.</p> <p>10 We are off the record.</p> <p>11 (Whereupon, a break for lunch was taken</p> <p>12 from 12:52 p.m. to 1:49 p.m.)</p> <p>13 THE VIDEOGRAPHER: The time right now</p> <p>14 is 1:49 p.m.</p> <p>15 We're back on the record.</p> <p>16 BY MR. CARNEY:</p> <p>17 Q. Good afternoon, Doctor.</p> <p>18 Over the break, did you have any</p> <p>19 substantive discussions about the case or the</p> <p>20 deposition with anyone?</p> <p>21 A. I did talk to the Latham team.</p> <p>22 Q. Okay. About the deposition?</p> <p>23 A. Yes.</p> <p>24 Q. All right. When we broke, you were</p> <p>25 looking at Exhibit 6, which was the samples of the</p> <p style="text-align: center;">138</p>	<p>1 Q. What does "below the level of</p> <p>2 analysis" mean?</p> <p>3 A. That, you know, the securities</p> <p>4 statement, you know, says that SolarWinds has</p> <p>5 certain processes and practices in place.</p> <p>6 And, you know, the approach I took to</p> <p>7 my assessment, you know -- you know, clearly</p> <p>8 indicated to me, just as in other instances, you</p> <p>9 know, that I've done this in the industry and</p> <p>10 observed others do it, that those were, you</p> <p>11 know -- that those were in place, things like the</p> <p>12 process for system access -- you know, implemented</p> <p>13 by the system access request for forms and the</p> <p>14 user access request.</p> <p>15 Q. Okay. So why don't we just quickly</p> <p>16 look at what was Exhibit 5, which was the</p> <p>17 securities statement.</p> <p>18 A. Uh-huh.</p> <p>19 Q. So on the page ending in 337108, which</p> <p>20 would be the second-to-last page.</p> <p>21 Do you see that?</p> <p>22 A. Okay. Yep.</p> <p>23 Q. And under "Access Controls," it says,</p> <p>24 "Role-based access." And so the first sentence</p> <p>25 says, "Role-based access controls are implemented</p> <p style="text-align: center;">140</p>

Gregory Rattray
2/12/2025

<p>1 for access to information systems."</p> <p>2 What is -- what does the SARFs in</p> <p>3 Exhibit 6 tell you about whether or not role-based</p> <p>4 access controls were implemented for access to</p> <p>5 information systems?</p> <p>6 A. I mean, this is part of a process of</p> <p>7 implementation for role-based access controls.</p> <p>8 Q. Okay. Is there anything about the</p> <p>9 SARFs standing alone that tell you that the access</p> <p>10 controls were actually implemented?</p> <p>11 A. You know, there was a -- I mean, the</p> <p>12 issue is the SARFs don't standalone, right?</p> <p>13 There's policy, there's the deposition testimony</p> <p>14 of leaders, you know, that goes into detail about</p> <p>15 how this access control was implemented.</p> <p>16 There are SARFs is one of the</p> <p>17 mechanisms that are used along with user access</p> <p>18 requests so -- as well as the fact that outside</p> <p>19 auditors all looked at the same control set and</p> <p>20 validated it was in place.</p> <p>21 So, you know, the SARFs are not an</p> <p>22 isolated piece of data related to role-based</p> <p>23 access control -- or, you know -- yeah.</p> <p>24 Q. Okay. And the reason I asked that is</p> <p>25 because earlier in response to one of my questions</p> <p style="text-align: center;">141</p>	<p>1 you one more question about that -- one more</p> <p>2 sentence in that paragraph. The third sentence</p> <p>3 says, "Access controls to sensitive data in our</p> <p>4 database's systems and environments are set on a</p> <p>5 need-to-know/least privilege necessary basis."</p> <p>6 Is there anything about the SARFs that</p> <p>7 we're looking at in Exhibit 6 that show you that</p> <p>8 statement that I just read you about the need to</p> <p>9 know least privileged necessary base was followed?</p> <p>10 A. Well, again, the SARFs are, again,</p> <p>11 part of a system of implementation about need to</p> <p>12 know and privilege.</p> <p>13 You know, they -- they do provision.</p> <p>14 You know -- they're part of the process of</p> <p>15 provisioning a user with a proper, you know,</p> <p>16 access at the least privilege necessary level.</p> <p>17 Q. So you would agree then that SARFs and</p> <p>18 the tickets alone don't demonstrate that the</p> <p>19 securities statement was followed with respect to</p> <p>20 access controls, right?</p> <p>21 MR. TURNER: Object to form.</p> <p>22 Mischaracterization of testimony.</p> <p>23 THE WITNESS: As I said, the SARFs and</p> <p>24 the user access -- yeah, the user access request</p> <p>25 can't -- can't be taken in isolation in evaluating</p> <p style="text-align: center;">143</p>
<p>1 you said that the SARF process and the user access</p> <p>2 request -- and you said you note tickets really</p> <p>3 demonstrated what the securities statement called</p> <p>4 for.</p> <p>5 So are you saying that you need to</p> <p>6 look at more than the SARF and the tickets to see</p> <p>7 whether this -- what the security statement called</p> <p>8 for was followed?</p> <p>9 A. I think what I'm saying is, you know,</p> <p>10 the SARFs and user access controls were among the</p> <p>11 data that I used, you know, to -- example, you</p> <p>12 know, the presence or practice around role-based</p> <p>13 access.</p> <p>14 As I've said many times, I used -- you</p> <p>15 know, common, you know, approach in the industry</p> <p>16 of, you know, looking for policy and procedure,</p> <p>17 you know, talking to or looking at depositions of</p> <p>18 management about how they implemented these</p> <p>19 things, artifacts like the SARFs and the UARs.</p> <p>20 And, you know, the fact that in many</p> <p>21 cases, outside audits also look at the same</p> <p>22 controls. So, you know, that -- it was the</p> <p>23 approach that I took across all of the areas that</p> <p>24 I evaluated.</p> <p>25 Q. Okay. And, Doctor, let me just ask</p> <p style="text-align: center;">142</p>	<p>1 a part -- you know, an aspect of the security</p> <p>2 statement.</p> <p>3 And there's a much richer set of</p> <p>4 evidence about the presence of these controls that</p> <p>5 I did use.</p> <p>6 BY MR. CARNEY:</p> <p>7 Q. Okay. So can you, maybe just to</p> <p>8 clarify for me, why it wasn't necessary to look at</p> <p>9 the specific tickets associated with these SARFs</p> <p>10 you used as examples?</p> <p>11 A. You know, as is typical, when, you</p> <p>12 know, people are assessing something like the</p> <p>13 practices, you know, there's a rich set of</p> <p>14 evidence which, you know, I can, again, repeat in</p> <p>15 terms of the presence of policy, clear deposition</p> <p>16 statements about how that was executed by</p> <p>17 management, strong documentation, you know, SARFs,</p> <p>18 user access.</p> <p>19 Again, auditors also looking at these</p> <p>20 process and saying there was sufficient evidence</p> <p>21 to say that these things were in place, you can't</p> <p>22 go down to the -- you know, the specific level on</p> <p>23 any specific form and, you know, and look at it.</p> <p>24 It's just beyond the scope of what was</p> <p>25 necessary to see that the securities statement</p> <p style="text-align: center;">144</p>

Gregory Rattray
2/12/2025

<p>1 depicted, you know, SolarWinds's conduct in a way 2 that the readers of the securities statement would 3 expect. 4 Q. All right. Sir, if I could ask you to 5 turn to page 20, paragraph 45. 6 A. Of -- yeah, my statement. I see. 7 Q. Yeah. Sorry. Of Exhibit 1. 8 A. Uh-huh. 9 Q. And you see there's a paragraph there, 10 paragraph 45 that talks about tickets. And if you 11 turn over to the next page, you say, "As with the 12 SARF forms, I have reviewed samples from thousands 13 of these tickets I received from the relevant 14 period evidencing that they were generated as a 15 regular process as part of the SARF process." 16 Do you see that? 17 A. Yeah. I just want to orient a bit. 18 Are we talking about the bottom of 19 page 21? 20 Q. So what I just read was from the top 21 of 21, and then it has a Footnote 36 at the bottom 22 that has the samples, I believe, of the tickets 23 that you selected; is that right? 24 A. I mean, what I'm reading is, "As with 25 the SARF form, I reviewed samples."</p> <p style="text-align: center;">145</p>	<p>1 (Whereupon, Exhibit 7 is marked for 2 identification.) 3 BY MR. CARNEY: 4 Q. All right. As with the SARFs from 5 Footnote 28, I put together the tickets from 6 Footnote 36 -- 7 A. Uh-huh. 8 Q. -- as one exhibit. And I'm not going 9 to go through all of them, but if we look at the 10 first page, the first ticket, do you know what 11 employee this relates to? 12 A. You know, in terms of, you know, which 13 employee, I don't know specifically. I assume, 14 you know, that it's Makins Rickey. But, you know, 15 I did not analyze each of these forms in detail. 16 I mean, I analyzed the nature of the 17 form, but I didn't look at the specific, you know, 18 data in each field of the form. 19 Q. Okay. And if we look at that first 20 page ending in 49602, down in the notes, if we 21 look at the bottom note, does it appear to relate 22 to someone named Mark Fraser? 23 A. Can you point me a little more 24 generally to what I'm looking for? 25 Q. Sure. Sure. If we look at the ticket</p> <p style="text-align: center;">147</p>
<p>1 Is that what you were quoting? 2 Q. Yes. 3 A. For me, that's on the bottom of 4 page 21, just to be -- just to be precise about 5 it. 6 Q. Are you looking at Exhibit 1? 7 A. Oh, you know what? I'm probably 8 looking at Exhibit 2. Sorry. 9 And the page reference? 10 Q. Page 21, please. 11 A. 21. 12 Q. 20 over to 21. 13 A. Okay. Yeah, I just want to make sure 14 I read the context for it properly. 15 Q. Sure. Of course. 16 (Pause for reading/reviewing.) 17 A. Okay. 18 Q. Similar to what I asked you earlier, 19 how were the samples that you have in Footnote 36 20 selected? 21 A. In a similar fashion as with the 22 SARFs. 23 Q. And I'll represent that I counted that 24 you have nine samples listed in Footnote 36. 25 A. Uh-huh.</p> <p style="text-align: center;">146</p>	<p>1 info in the subject line, it also mentions Mark 2 Fraser. 3 Do you see that? 4 A. Again, I -- which -- I may be looking 5 at the wrong -- 6 Q. On the first -- the first page. 7 MR. TURNER: It's right here. 8 THE WITNESS: Oh. 9 BY MR. CARNEY: 10 Q. 4960. 11 A. Okay. Yeah, well, I see an email down 12 at the bottom, two lines, the very bottom with an 13 email from Mark Fraser. 14 What else am I looking at here? 15 Q. I'm just wondering if that sort of 16 refreshes your recollection or helps you 17 understand that this ticket relates to Mark Fraser 18 rather than Rickey Makins? 19 A. That was, again, below the level that 20 I was looking at these, you know, tickets in this 21 case. 22 You know, the presence of the tickets 23 sort of clearly indicated that the things that 24 management said were in place, were in place in 25 terms of a process for role-based access and, you</p> <p style="text-align: center;">148</p>

Gregory Rattray
2/12/2025

<p>1 know, implementing that.</p> <p>2 You know, I did not -- did not feel it</p> <p>3 was necessary to look at the implementation in</p> <p>4 each specific example.</p> <p>5 Q. And just to be clear, I'm just talking</p> <p>6 about the nine examples --</p> <p>7 A. Uh-huh.</p> <p>8 Q. -- that you cited in your report.</p> <p>9 You didn't think it was necessary to</p> <p>10 look at those?</p> <p>11 A. I mean, I did look at them, and I</p> <p>12 selected them.</p> <p>13 Q. Okay. Can you tell what access level</p> <p>14 this employee was being given?</p> <p>15 A. I -- the person who would have</p> <p>16 received this would have been the person that</p> <p>17 needed to be able to, you know, interpret what</p> <p>18 each of these fields are.</p> <p>19 I'm very confident that, you know,</p> <p>20 this process, you know, allowed, you know, the</p> <p>21 recipient of a user access, you know, request to,</p> <p>22 you know, conduct the process properly.</p> <p>23 You know, as you can see, the forms</p> <p>24 are complicated and -- you know, I wasn't trained</p> <p>25 as a SolarWinds, you know, recipient of this</p> <p style="text-align: center;">149</p>	<p>1 assumption that they would do all this for -- you</p> <p>2 know, and not actually conduct all the activity.</p> <p>3 These processes are heavy weight and, you know, in</p> <p>4 place in order to accomplish what was in the</p> <p>5 security statement.</p> <p>6 And it's pretty clear that, you know,</p> <p>7 the reader of the security statement would</p> <p>8 understand that, you know, SolarWinds was doing,</p> <p>9 you know -- meeting the representations in the</p> <p>10 security statement.</p> <p>11 Q. In your mind, is having a process in</p> <p>12 place mean that the process is followed?</p> <p>13 A. Is this a hypothetical question?</p> <p>14 Q. Not really. It's just I'm wondering</p> <p>15 if you see that --</p> <p>16 A. I mean, just in general outside of</p> <p>17 this specific situation?</p> <p>18 Q. Yes.</p> <p>19 A. And, again, could you create a process</p> <p>20 document and do nothing to implement it? That's</p> <p>21 possible. But it's clearly not the case in what</p> <p>22 we see here with SolarWinds.</p> <p>23 Even these documents, which are not</p> <p>24 process documents, they're implementation</p> <p>25 documents demonstrate, you know, efforts to</p> <p style="text-align: center;">151</p>
<p>1 ticket, so I don't know exactly.</p> <p>2 Q. Did you look at the SARF associated</p> <p>3 with this particular ticket?</p> <p>4 A. No. I didn't feel like I needed to.</p> <p>5 But I was looking for in both cases, the SARF</p> <p>6 process and these tickets, was the existence of</p> <p>7 the process which clearly demonstrated SolarWinds</p> <p>8 had a role-based access approach that, you know,</p> <p>9 was utilized in order to, you know, appropriately</p> <p>10 provision access.</p> <p>11 Q. How does the existence of the process</p> <p>12 tell you that it was appropriately used?</p> <p>13 A. Well, you know, again, I didn't rely</p> <p>14 solely on the artifacts that showed existence of</p> <p>15 the process.</p> <p>16 There was testimony by the management</p> <p>17 under oath and depositions that the process was</p> <p>18 being conducted. There were other outside</p> <p>19 assessments that also found the same.</p> <p>20 So, you know, as we've been talking</p> <p>21 about quite a bit, the assessment I did, it wasn't</p> <p>22 necessary to get to the level of, you know,</p> <p>23 mapping each individual, you know, ticket to its</p> <p>24 execution, because I don't think that's necessary.</p> <p>25 I mean, we're sort of making the</p> <p style="text-align: center;">150</p>	<p>1 implement the process.</p> <p>2 Q. And you said could you create a</p> <p>3 process document and do nothing to implement it.</p> <p>4 How about could you create a process</p> <p>5 document and not implement it correctly? Is that</p> <p>6 possible?</p> <p>7 A. Again, we're sort of abstracting out</p> <p>8 of any specific in the SolarWinds case?</p> <p>9 Q. Yes.</p> <p>10 A. Yes. Improper process implementation</p> <p>11 is theoretically possible.</p> <p>12 Q. And in the case of -- let's use the</p> <p>13 SolarWinds SARF ticket process.</p> <p>14 What would you have had to have seen</p> <p>15 to know whether or not the process was being</p> <p>16 implemented improperly?</p> <p>17 A. You know, again, my assignment was to</p> <p>18 sort of evaluate the security statement and, you</p> <p>19 know, assess whether the things that were, you</p> <p>20 know, asserted there were in place.</p> <p>21 You know, clearly, you know, the</p> <p>22 presence of, you know, not just process</p> <p>23 documentation but many, many artifacts of</p> <p>24 implementation indicated that the process was</p> <p>25 there.</p> <p style="text-align: center;">152</p>

<p>1 It wasn't my role to look at sort of 2 at the granular level, you know, the implement -- 3 the exact implementation of it in detail. I 4 mean -- you know, at an instance-by-instance 5 detail. 6 Q. So is it fair to say that at a high 7 level, in this case, you're offering the opinion 8 that during the relevant period, as you've defined 9 it, the SolarWinds security statement was not 10 inaccurate or misleading? 11 A. It is my opinion that the SolarWinds 12 security statement was -- was accurate. 13 Q. Okay. And it's your opinion that by 14 virtue of that, this securities statement was not 15 misleading? 16 A. Yeah, I do not believe the security -- 17 the SolarWinds security statement was misleading, 18 no. 19 Q. Is it fair to say that's sort of the 20 crux of your expert opinion? 21 A. You know, the crux of my expert 22 opinion was, you know, as detailed in my expert 23 report. I looked at the security statement, you 24 know, focused on particular areas that I -- you 25 know, believe are at issue in the case.</p> <p>153</p>	<p>1 A. Okay. 2 Q. Okay. Sir, in the last sentence of 3 paragraph 49 you say, "Again, I have samples from 4 numerous SARFs I received requesting such changes 5 along with corresponding tickets evidencing that 6 this practice was commonly followed during the 7 relevant period." 8 So I want to ask you about that. 9 What does it mean that it was commonly 10 followed? 11 A. Again, with the SARF that I received 12 with tickets, it looks like they were executing 13 the practice, which was the level at which I was 14 trying to, you know, see that direct evidence of 15 the practice and implementation. 16 That, you know, I was not looking to 17 statistically analyze the full -- the full set, 18 you know. So commonly followed was -- with the 19 evidence I saw, it was followed. 20 Q. When you say you were "not looking to 21 statistically analyze the full set," what do you 22 mean by that? 23 A. Well, I think it sort of -- I didn't 24 look at every SARF related to a change, and all of 25 the corresponding tickets and -- and do a</p> <p>155</p>
<p>1 And, you know, saw evidence of a 2 variety -- you know, variety of sorts that 3 indicated the assertions made in the security 4 statement were true. 5 Q. All right. Sir, if I could ask you to 6 turn to page 23, paragraph 49. 7 A. Uh-huh. 8 MR. TURNER: Can you just give me a 9 minute, Chris. I'm having trouble tracking down 10 Exhibit 1. 11 MR. CARNEY: Oh, I might have another 12 copy, if you want. 13 THE WITNESS: Did I steal that one 14 too? I don't think so. 15 (Whereupon, discussion held off the 16 written record to find document.) 17 THE WITNESS: Exhibit 1 again. 18 BY MR. CARNEY: 19 Q. Yes, sir. So page 23, paragraph 49. 20 A. Okay. You know, may I have a quick 21 moment to just read the paragraph? 22 Q. Of course. Anytime you need that, 23 just -- 24 A. Okay. 25 (Pause for reading/reviewing.)</p> <p>154</p>	<p>1 statistical analysis, because it was unnecessary 2 as we've assessed quite a bit. 3 You know, the process -- you know, the 4 clear, deep, you know, documents -- you know, 5 documentary evidence that they had these processes 6 and they were doing them is the level at which my 7 analysis was conducted and is -- you know, the 8 level of analysis that I think would be expected 9 in terms of the security statement. 10 Q. Okay. And you'd agree, commonly 11 followed doesn't mean uniformly followed, right? 12 A. If you're asking that, you know -- is 13 the question that -- I'm just trying to 14 understand -- 15 Q. Sure, sure. 16 A. -- you know, is the question that -- 17 whether, you know, I'm asserting by saying 18 "commonly followed" that every -- every SARF or, 19 you know, for change was done perfectly? 20 Because, yeah, it definitely doesn't 21 mean that they achieved the standard of 22 perfection. 23 Q. Okay. And just picking up on your 24 comment about not having done a statistical 25 analysis, so it's fair to say you didn't look to</p> <p>156</p>

Gregory Rattray
2/12/2025

<p>1 see what percentage of the time this process was 2 followed, right? 3 MR. TURNER: Object to form. 4 THE WITNESS: You know, we've 5 discussed this a lot, and I've -- we may do it 6 quite a bit this afternoon. That was out -- you 7 know, outside the scope on the sense that, you 8 know, I had multiple sources of information that, 9 you know, clearly indicated -- you know, that 10 SolarWinds was doing the practices, in this case, 11 proper role-based access control that the 12 securities statement; and, therefore, you know, I 13 did not do an analysis of, you know, every 14 instance of the SARFs across the entire relevant 15 period. 16 BY MR. CARNEY: 17 Q. Okay. And let me just ask you a 18 hypothetical then -- 19 A. Uh-huh. 20 Q. -- this is not SolarWinds, just a 21 hypothetical. 22 If the access -- companies' user 23 access policy was followed 95 percent of the time, 24 but the 5 percent of the time that it was not 25 followed involved elevated permissions being</p> <p style="text-align: center;">157</p>	<p>1 affirmed they were performing in the security 2 statement. 3 BY MR. CARNEY: 4 Q. Okay. All right. 5 (Whereupon, Exhibit 8 is marked for 6 identification.) 7 BY MR. CARNEY: 8 Q. All right. Doctor, you've been handed 9 what's been marked as Exhibit 8. And I'll 10 represent to you that these are the -- in that 11 last sentence of paragraph 49 we just looked at, 12 you say that you, "have samples from numerous 13 SARFs I received requesting such changes along 14 with the corresponding tickets." 15 And that -- so these appear to be the 16 samples that are in Footnote 44 -- 17 A. Okay. 18 Q. -- do you see that? 19 A. Yes. 20 Q. And so first of all, would you -- if 21 you could just flip through this -- 22 A. Uh-huh. 23 Q. -- are all these documents tickets or 24 any of them SARFs, as you understand, in your 25 Footnote 44?</p> <p style="text-align: center;">159</p>
<p>1 granted to employees who should not have had them, 2 would your opinion change about whether the -- 3 following it -- what's the word? I'm sorry, let 4 me -- whether following it commonly was enough? 5 MR. TURNER: Object to form. 6 THE WITNESS: Again, you know, the 7 statement we've been reading this last sentence of 8 paragraph 49 is not the sole basis for my, you 9 know -- you know, my assessment that SolarWinds's 10 security statement related to role-based access is 11 correct. 12 There's many, many other sources of 13 information that sort of indicated that they were 14 doing the things that there are in the security 15 statement. 16 You know, in terms of a statistical -- 17 you know, the 95/5, I mean, it's very 18 hypothetical. I would have to understand a lot of 19 context around the company of concern, you know, 20 again -- you know, the -- the errors in why that 21 error rate. 22 But that was out of scope for, you 23 know, the exercise here, which was to look at the 24 securities statement and, you know, assess whether 25 SolarWinds was, you know, performing as they</p> <p style="text-align: center;">158</p>	<p>1 MR. TURNER: I'm just confused. The 2 footnote is citing what I assume are SARFs, and 3 then it says, "I understand the tickets have been 4 produced with the corresponding SARFs attached." 5 Maybe I read it backwards, but... 6 MR. CARNEY: Right. So I'm just -- 7 MR. TURNER: The footnote is 8 referencing both, and there's obviously 9 attachments missing here. 10 MR. CARNEY: You say there's 11 attachments missing. 12 MR. TURNER: It says -- the footnote 13 says, "I understand the tickets have been produced 14 with the corresponding SARF forms attached." 15 So if these are the tickets, I assume 16 there were SARF forms attached to the production, 17 and they're missing here. 18 MR. CARNEY: Okay. 19 BY MR. CARNEY: 20 Q. All right. And you can -- you can 21 look through -- you can look through the Bates 22 numbers that are cited in Footnote 44 and tell me 23 if I'm missing any of the documents that you cite 24 to in that footnote. 25 MR. TURNER: We can go off the record</p> <p style="text-align: center;">160</p>

Gregory Rattray
2/12/2025

1 if you like. I think, Maurice maybe can explain
2 this.

3 But I think basically if you -- the
4 way the documents were electronically produced,
5 the SARFs were an attachment to the document just
6 like with an email.

7 MR. BAYNARD: I believe the tickets
8 were produced earlier and then we produced the
9 SARF form [indiscernible].

10 THE STENOGRAPHER: I can't hear you.

11 MR. BAYNARD: That we produced the
12 SARF forms later with an overlay so they were
13 linked in the review database so you could see the
14 attached ticket -- further attached form to each
15 ticket.

16 MR. CARNEY: Okay.

17 BY MR. CARNEY:

18 Q. And with that --

19 MR. TURNER: So there was no way -- I
20 just -- to clarify, so I'm not sure there's a way
21 of citing to SARFs directly.

22 MR. CARNEY: So you're saying they
23 don't have Bates numbers, is what --

24 THE WITNESS: That may be.

25 MR. BAYNARD: They have Bates numbers,

161

1 followed the process that Mr. Baynard described
2 and looked at the associated SARFs?

3 MR. TURNER: If -- just to make the
4 record clear, I think that what happened is the
5 documents were produced to Mr. Rattray before they
6 were produced to y'all in the form we just
7 discussed.

8 So he may have gotten the tickets with
9 the SARFs attached, but in order to produce them
10 to you, the tickets had already been produced, so
11 we were overlaying them with those so they
12 wouldn't appear as attachments. It's complicated.

13 MR. CARNEY: Okay.

14 MR. TURNER: But as far as I
15 understand, Mr. Rattray would have received them
16 originally as tickets, and attached --

17 (Simultaneous unreportable crosstalk
18 occurs among parties.)

19 THE WITNESS: And I would have
20 reviewed that as a group, if they were -- if the
21 SARFs were attached to the tickets.

22 BY MR. CARNEY:

23 Q. Okay. And do you recall whether the
24 SARFs were attached to the tickets when you looked
25 at these samples?

163

1 but they just aren't sequential, because they were
2 produced at a later date.

3 MR. CARNEY: Okay. And thank you for
4 that clarification.

5 BY MR. CARNEY:

6 Q. So, Doctor, would you have looked at
7 the SARFs that are associated with the tickets
8 that are listed in Footnote 44?

9 A. Yes. As we were just discussing, you
10 know, as these -- as this evidence was produced,
11 you know, I looked at it.

12 I don't know that I can map each one
13 of these to the SARF, but, you know, there is a --
14 you know, again, I think we just heard, there's a
15 process for that.

16 But, you know, again, I clearly looked
17 at these tickets, you know, to the notion of this
18 paragraph, which is there was an implementation,
19 you know, in place for the change process.

20 I think if you read through these,
21 it's pretty clear that they were implementing --
22 you know -- they were implementing changes to --
23 you know, role-based changes.

24 Q. Okay. And I was really just trying to
25 understand from a technical standpoint if you

162

1 A. You know, I believe they were. But,
2 again, as you can -- you know, you can well see,
3 there was a lot of evidence we were working
4 through.

5 Again, my assignment was to make sure
6 that the tickets in this case from SARFs related
7 to changes, that the process -- you know, the
8 SARFs generated tickets and the tickets were acted
9 upon.

10 Q. Okay. All right. And once again, I
11 don't want to go through all these tickets, so
12 let's just use one as an example. If we look at
13 the first page --

14 A. Uh-huh.

15 Q. -- ending in 47323, can you tell what
16 type of access request change is being made here?

17 MR. TURNER: Just take your time --

18 THE WITNESS: Yeah --

19 MR. TURNER: -- to read through the
20 document.

21 THE WITNESS: -- uh-huh.

22 Again, as we look at what, you know,
23 this filled out ticket, you know -- where, again,
24 I was looking at not any specific access change
25 but the presence of a process and, you know, an

164

<p>1 implementation of a process for ticketing to make 2 sure the changes got done. 3 You know, I read a sentence that 4 please note that Andy is not [indiscernible]. 5 THE STENOGRAPHER: I can't understand 6 you. 7 THE WITNESS: Okay. Yeah. So as I 8 read this, there's a sentence that says, "Please 9 note that Andy is now an employee of SolarWinds 10 MSP UK. Can his access be amended to reflect the 11 change from contractor to employee?" 12 So I believe, you know, that would 13 probably be the -- you know, the access change 14 requested. 15 BY MR. CARNEY: 16 Q. And what's the difference in access 17 from a contractor to an employee at SolarWinds? 18 MR. TURNER: Objection. Foundation. 19 THE WITNESS: You know, I don't know 20 the specifics of what systems contractors get 21 versus employees. 22 As we've talked about a lot, it's 23 clear that SolarWinds had a process to control and 24 properly provision role-based access, and that's 25 what I was looking for.</p> <p style="text-align: center;">165</p>	<p>1 finish -- 2 Q. Okay. 3 A. -- but why don't you please proceed. 4 Q. Sure. 5 So I just read that -- that paragraph 6 to you. I won't read -- 7 A. Yeah. You don't need to read it 8 again -- 9 Q. -- it again? 10 A. -- but the first two sentences of 11 paragraph 52. 12 Q. Got it. 13 And then you quote from the security 14 statement regarding access controls. 15 Let me just focus you on the last 16 sentence -- 17 A. Uh-huh. 18 Q. -- it says, "Access controls to 19 sensitive data in our database systems and 20 environments are set on a need-to-know/least 21 privilege necessary basis." 22 How -- you state in paragraph 52 that 23 the artifacts you looked at easily demonstrate 24 that the representations in the securities 25 statement relating to role-based access controls</p> <p style="text-align: center;">167</p>
<p>1 BY MR. CARNEY: 2 Q. All right. Sir, if I could -- you can 3 put that one aside. 4 A. Uh-huh. 5 Q. If I could ask you to turn to page 24. 6 You state -- and you can -- if you need -- at any 7 time, if you need to read back to get context -- 8 A. Uh-huh. 9 Q. -- please feel free, but it says, "All 10 these are the source of artifacts I would look for 11 had I been hired in the ordinary business context 12 to conduct an assessment of SolarWinds's 13 role-based access controls. 14 "In my opinion, they easily 15 demonstrate that the representations in the 16 securities statement relating to role-based access 17 controls were true." 18 And then you -- 19 A. I'm just trying to -- I'm actually not 20 tracking where you are reading. 21 Q. Oh, sorry. I'm on page 24. 22 A. Exhibit 1. 23 Q. Exhibit 1. Paragraph 52. 24 A. Okay. Got it. I'm now seeing it. 25 Yeah. I may read this contextually when you</p> <p style="text-align: center;">166</p>	<p>1 were true. 2 And can you just explain to me how 3 these samples that we just looked at easily 4 demonstrate to you that SolarWinds was only 5 allowing access on a need-to-know/least privilege 6 necessary basis? 7 MR. TURNER: Object to form. 8 Mischaracterization. 9 Go ahead. 10 THE WITNESS: Okay. The whole SARF 11 process where, you know, role-based access is 12 basically the same as need-to-know, right? 13 So, you know, we've had the discussion 14 about these SARFs and tickets that I've reviewed, 15 you know, being -- you know, among the evidence I 16 used for role-based access, and, again, which is 17 synonymous with need-to-know. 18 So, you know, that's why I made -- 19 that's why I'm confident in this statement. 20 BY MR. CARNEY: 21 Q. And just to make sure I'm 22 understanding, the individual SARFs and tickets 23 that you looked at by themselves don't demonstrate 24 to you that the representations in the securities 25 statement relating to role-based access controls</p> <p style="text-align: center;">168</p>

Gregory Rattray
2/12/2025

<p>1 were true, right?</p> <p>2 MR. TURNER: Object to form.</p> <p>3 THE WITNESS: I've answered, I</p> <p>4 believe, this -- pretty much the same question,</p> <p>5 right?</p> <p>6 That the SARFs -- and, you know, the</p> <p>7 associated tickets were an element of a -- you</p> <p>8 know, an element of a system and a set of, you</p> <p>9 know -- a subset of their total amount of data</p> <p>10 that I used to, you know, make the assertion that</p> <p>11 all of these are the sorts of artifacts I would</p> <p>12 look for, right?</p> <p>13 So I looked for these for presence of</p> <p>14 implementation in the form of, you know, a</p> <p>15 process, which the SARF -- the SARFs show how they</p> <p>16 did. System access request and the tickets show</p> <p>17 how that was -- you know, how that moved through</p> <p>18 to the implementation.</p> <p>19 So, you know....</p> <p>20 So that is how I made -- you know,</p> <p>21 made the judgment in this case.</p> <p>22 BY MR. CARNEY:</p> <p>23 Q. Can you have role-based access that is</p> <p>24 not synonymous with a need-to-know basis?</p> <p>25 A. Are we talking about some sort of</p> <p style="text-align: center;">169</p>	<p>1 next page.</p> <p>2 A. Yep.</p> <p>3 Q. And in that paragraph, you discuss</p> <p>4 user access reviews.</p> <p>5 Do you see that?</p> <p>6 A. I'm going to read the paragraph --</p> <p>7 Q. Sure.</p> <p>8 A. -- so -- yeah, just so we can proceed</p> <p>9 when I have enough context.</p> <p>10 (Pause for reading/reviewing.)</p> <p>11 (Whereupon, Exhibit 9 is marked for</p> <p>12 identification.)</p> <p>13 THE WITNESS: Yeah, I've read</p> <p>14 paragraph 53.</p> <p>15 BY MR. CARNEY:</p> <p>16 Q. And in Footnote 51, you cite a number</p> <p>17 of samples of user access reviews that you looked</p> <p>18 at, right?</p> <p>19 A. Yes.</p> <p>20 Q. Okay. I -- all right. And I'll just</p> <p>21 tell you this Exhibit 9, I think this was printed</p> <p>22 out in the native format, so it doesn't have the</p> <p>23 Bates number on it, but this would be the first</p> <p>24 sample in Footnote 51, which is SW-SEC-00296522.</p> <p>25 A. Yes.</p> <p style="text-align: center;">171</p>
<p>1 hypothetical situation?</p> <p>2 Q. Yes.</p> <p>3 A. Yeah, probably want to avoid any kind</p> <p>4 of given hypothetical. But role-based access is</p> <p>5 the way companies, you know, as common practice</p> <p>6 and language now, you know, handle access</p> <p>7 controlling.</p> <p>8 And, you know, in the case of the</p> <p>9 securities statement, you know, that's the</p> <p>10 expectation of the reader of the securities</p> <p>11 statement and, you know, vendor management teams</p> <p>12 is to see that a company like SolarWinds, when</p> <p>13 you're buying their products, you know,</p> <p>14 understands that they need to have role-based</p> <p>15 access in place.</p> <p>16 I mean, that's what the purpose of</p> <p>17 this statement is, and that is why I examined what</p> <p>18 I examined.</p> <p>19 Q. All right. Sir, if I could direct</p> <p>20 your attention to paragraph 53, which is on</p> <p>21 page 25 of Exhibit 1.</p> <p>22 A. Okay. Sorry. I went to -- before all</p> <p>23 I should say, remember, Greg, it's paragraph 53</p> <p>24 not page 53. I'm there, paragraph 53.</p> <p>25 Q. Okay. And then it goes over on to the</p> <p style="text-align: center;">170</p>	<p>1 Q. And have you looked at this particular</p> <p>2 user access review before?</p> <p>3 A. You know, the user access reviews</p> <p>4 cited in Footnote 51, I looked through each of</p> <p>5 those.</p> <p>6 I mean, basically clicked through, you</p> <p>7 know, extensive set of, you know, user access</p> <p>8 reviews, right? Do I remember, you know, that</p> <p>9 this one is Bates numbered -- each particular</p> <p>10 Bates number here, I do not.</p> <p>11 Q. I would not expect that, sir.</p> <p>12 But the format of this, does this look</p> <p>13 familiar --</p> <p>14 A. Yes.</p> <p>15 Q. -- to user access reviews you looked</p> <p>16 at?</p> <p>17 Okay. Can you tell from looking at</p> <p>18 this user access review who conducted it?</p> <p>19 A. Let me just take a quick look through</p> <p>20 the whole thing.</p> <p>21 You know, in terms of who conducted</p> <p>22 it, you know, I think one perspective on the</p> <p>23 question is "who" might not be the right word.</p> <p>24 Because user access reviews are</p> <p>25 probably generated as a -- I mean, in many places</p> <p style="text-align: center;">172</p>

1 are generated as a normal set of data production
2 out of an automated system in order to make sure
3 that you're reviewing who had access, right?

4 So, you know, especially the -- you
5 know, the deep long, you know, fields and fields
6 of data that we see are clearly, you know, outputs
7 from, you know, an automated logging system.

8 So I'm not sure there's a single who
9 associated with the generation of this.

10 But what I was looking for was, you
11 know -- and, again, you know, as the -- as the
12 paragraph says, you know, as we'd talked about
13 SARFs and user access forms, the fact of regular
14 user access -- you know, regular review of user
15 access rights is just an additional layer of
16 confirmation for the processes, you know, outlined
17 in the securities statement.

18 **Q.** Okay. So rather than who conducted
19 it, what system was used to generate this user
20 access review?

21 **A.** You know, I asked for production of,
22 you know, data related to -- you know, role-based
23 access control, and user access reviews were
24 highlighted as one of the sources of information
25 that showed the implementation of the processes.

173

1 So in terms of the exact way these
2 were generated, I did not and felt like it was not
3 necessary to understand that. Having seen many
4 types of document -- process documentation, this
5 looks very clean and organized.

6 And to the extent to which, you know,
7 do I feel this provides good granularity and
8 ongoing confidence that SolarWinds reviewed the
9 access their users had, this data set, you know,
10 to me very clearly indicates that that was the
11 case.

12 **Q.** And what makes this data set clean?

13 **A.** Just well organized, right? You know,
14 in terms of, you know, the fields that are in
15 here, the account types that are in here.

16 You know, again, cleaning and pretty
17 comprehensive, right? You know, the locations,
18 the names, the email addresses, right?

19 You know, in terms of, you know,
20 output that would, you know, show that a process
21 existed in addition to the, you know, SARF and,
22 you know, user access ticketing process that
23 they're actually reviewing it and confirming that
24 their role-based access program was in place, this
25 is good documentation of that.

174

1 **Q.** And what, if any, conclusions can you
2 draw about whether user access was only allowed on
3 a need-to-know/least privilege necessary basis
4 from looking at user access reports like this?

5 **A.** You know, again, the assertion that I
6 made in the -- regarding the security statement in
7 terms of need-to-know and least privileged was the
8 presence of the system that, you know, the
9 role-based access system of which this is just one
10 cross-check on that system.

11 And so, you know, these user access
12 reviews allowed -- you know, would allow for
13 checking whether the process of, you know,
14 provisioning of users was -- you know, the data
15 there to check that it was done properly.

16 **Q.** Okay. All right. Sir, if I could ask
17 you to please turn to page 65 of your report.

18 In paragraph 119, it starts at the
19 bottom. And you can look at paragraph 118 might
20 be help -- provide some context too.

21 **A.** Uh-huh.

22 **Q.** You're talking about a help desk
23 ticket that Mr. Graff cited.

24 Do you recall that?

25 **A.** Yeah. If it's okay, I just would like

175

1 to read 18, 19 --

2 **Q.** Sure.

3 **A.** -- and maybe 20 just so I get the full
4 context?

5 **Q.** Of course.

6 (Pause for reading/reviewing.)

7 **A.** Okay. I think I'm ready.

8 **Q.** All right. So if you look -- now that
9 you have the context, if you look in
10 paragraph 119, the second sentence, you say,
11 "First, it's not even clear from the chat that the
12 one-year time period was incorrect. The person
13 who specified the time period may have gotten it
14 from the temps manager."

15 I want to stop right there.

16 Have you seen any documents indicating
17 that the person who specified the time period got
18 it from the temps manager?

19 **A.** Well, first, shouldn't we be looking
20 at the artifact we're talking about here?

21 **Q.** If you would like to, sure.

22 **A.** Yeah, I mean, that would be useful.
23 (Whereupon, Exhibit 10 is marked for
24 identification.)

25 MR. CARNEY: And just for the record,

176

1 I've handed you Exhibit 10. And that is the
2 artifact that you requested, and it's Bates number
3 SW-SEC-SDNY_00050922.

4 THE WITNESS: Okay. Yeah, I got the
5 artifact.

6 BY MR. CARNEY:

7 Q. Okay. So my question was: In
8 paragraph 119 of your report, you say, "The person
9 who specified the time period may have gotten it
10 from the temps manager."

11 And I asked: Have you seen any
12 evidence to that effect?

13 A. You know, I think, you know, in the --
14 the general context here, that the point being
15 made in that sentence is there are a lot of
16 explanations for what might or might not be on
17 this form.

18 But that this is one form out of
19 thousands of, you know, SARFs. And the specifics
20 here, which, again, I've said, you know, I was
21 trying to illuminate that, you know, we don't know
22 exactly how any specific form, you know, would be
23 filled out.

24 In terms of the question, have I seen,
25 you know, evidence that the -- you know, that

177

1 the -- that the person who needed the time period
2 defined could have gotten it from the temps
3 manager, I have not seen such evidence.

4 But as we've talked a lot about, I
5 didn't go to that level of analysis. I was sort
6 of asserting here or saying here, there's a lot of
7 reasons that this form could have been filled out
8 the way it is.

9 Q. Okay. So when you make the statement,
10 "The person who specified the time period may have
11 gotten it from the temps manager," you were
12 speculating; is that fair?

13 A. Oh, yeah. You know, it was sort of
14 with a distant illustration of, you know, more
15 fundamentally by focusing on this particular, you
16 know, ticket.

17 You know, the fact that a SARF has,
18 you know, ambiguity at this level is not the level
19 I was operating on for this assessment.

20 It's that they had a SARF process,
21 right? If you look -- if you look at the SARF and
22 the dialogue, it shows that they're trying hard to
23 figure out what is appropriate access, right?

24 Like, they're not just willy-nilly
25 implementing things. There's a dialogue with

178

1 notes. That is, you know, strong implementation
2 of a -- you know, a role-based access and control
3 system.

4 Q. All right. So instead of focusing on
5 the one ticket, in the second part of that
6 sentence in paragraph 119, you say, "Or that
7 period may have been a standard employment period
8 for a temp."

9 Do you see that?

10 A. I do.

11 Q. Okay. Have you seen any documents
12 among the thousands of SARF tickets you had access
13 to indicating that the one-year period was a
14 standard employment period for a temp?

15 A. This is a -- I think another example
16 of I wasn't looking for documentation at that
17 level. This was just illustrative of why there
18 might -- you know, what might be going on, you
19 know, in the case of this SARF.

20 And, again, to illuminate the fact
21 that they had a very strong process. And that,
22 you know, there wasn't a need at my -- you know,
23 for me to see if they had a role-based access
24 control process, like, stated in the securities
25 statement to look for that level of sort of

179

1 procedure -- you know, procedural execution.

2 Q. Okay. So is it fair to say that when
3 you said the period may have been a standard
4 employment period for a temp, that you were
5 speculating?

6 MR. TURNER: Object to form.

7 He's already explained the purpose of
8 the remark.

9 THE WITNESS: Yes. And as you know, I
10 can repeat the entire statement I just made.
11 Hopefully the record will -- you know, will show
12 that that wasn't my task to determine, you know,
13 all the specific procedural implementation.

14 This paragraph was meant to say, in
15 any specific case, you know, there may be good
16 reasons for why this SARF is the way it is. But
17 more fundamentally, they had a SARF process.

18 This SARF indicates a strong effort to
19 make sure that it was implemented in a thoughtful
20 way. And that was sufficient for me to affirm
21 what was in the securities statement.

22 BY MR. CARNEY:

23 Q. Okay. In that same paragraph towards
24 the end, you mentioned that, "A separate SARF
25 would be submitted upon an employee's

180

Gregory Rattray
2/12/2025

<p>1 termination."</p> <p>2 Do you see that?</p> <p>3 A. I do.</p> <p>4 Q. Have you seen the SARF ticket</p> <p>5 decommissioning this temp's access after they left</p> <p>6 the company?</p> <p>7 MR. TURNER: Objection. Assumes facts</p> <p>8 not in evidence.</p> <p>9 THE WITNESS: You know, I think</p> <p>10 we're -- we're gonna have the same conversation</p> <p>11 once again. You know, the point of paragraph 119</p> <p>12 is that -- to show that there's a lot of reason</p> <p>13 any individual SARF may have been written the way</p> <p>14 it is.</p> <p>15 But my -- you know, my expert report,</p> <p>16 you know, starts the next paragraph with, "But</p> <p>17 more fundamentally."</p> <p>18 And this is the point; that one</p> <p>19 particular SARF is really not -- not relevant to</p> <p>20 judging whether SARFs or more generally the full</p> <p>21 set of evidence, you know, presented around the</p> <p>22 presence of role-based access is sufficient for me</p> <p>23 to determine that, you know, I feel confident that</p> <p>24 the securities statement is -- is accurate.</p> <p>25 ///</p> <p style="text-align: center;">181</p>	<p>1 And then, "In particular, I have</p> <p>2 reviewed a chat between Tim Brown and Eric</p> <p>3 Quitugua," and then you go on to describe the</p> <p>4 chat.</p> <p>5 Do you see that?</p> <p>6 A. I do. I'm just going to -- as we've</p> <p>7 been doing the last little while, I just want to</p> <p>8 make sure I've got the context for things as, you</p> <p>9 know, we go into your questions.</p> <p>10 MR. TURNER: Go ahead. Take the time</p> <p>11 you need for it.</p> <p>12 (Pause for reading/reviewing.)</p> <p>13 THE WITNESS: Okay. I think I'm good</p> <p>14 for a moment.</p> <p>15 BY MR. CARNEY:</p> <p>16 Q. And so you see paragraph 67, the chat</p> <p>17 you reference?</p> <p>18 A. Yes.</p> <p>19 Q. And Mr. Quitugua sends back a</p> <p>20 screenshot in the chat; is that right?</p> <p>21 A. Yes. I -- yeah.</p> <p>22 Q. Is that correct?</p> <p>23 A. Yes, it -- that's right. You know, it</p> <p>24 happened in 2017, which was quite a bit outside</p> <p>25 the relevant period, but, yeah, I see that.</p> <p style="text-align: center;">183</p>
<p>1 BY MR. CARNEY:</p> <p>2 Q. All right. Sir, I'm going to switch</p> <p>3 topics to -- I'm going to ask you some</p> <p>4 questions --</p> <p>5 THE WITNESS: Can I ask for a break?</p> <p>6 I have to go to the bathroom.</p> <p>7 MR. CARNEY: Sure, sure.</p> <p>8 THE WITNESS: How long have we been</p> <p>9 going?</p> <p>10 MR. TURNER: An hour.</p> <p>11 THE VIDEOGRAPHER: The time right now</p> <p>12 is 2:52 p.m.</p> <p>13 We're going off the record.</p> <p>14 (Whereupon, a recess was taken at</p> <p>15 2:52 p.m.)</p> <p>16 THE VIDEOGRAPHER: The time right now</p> <p>17 is 3:04 p.m.</p> <p>18 We're back on the record.</p> <p>19 BY MR. CARNEY:</p> <p>20 Q. Dr. Rattray, if I could ask you to</p> <p>21 please look at page 35 of Exhibit 1, paragraph 67.</p> <p>22 A. Okay.</p> <p>23 Q. You say, "There's clear evidence in</p> <p>24 the record that SolarWinds did enforce password</p> <p>25 complexity on active directory."</p> <p style="text-align: center;">182</p>	<p>1 Q. And so if it happened quite a bit</p> <p>2 outside the relevant period, why did you rely on</p> <p>3 that chat?</p> <p>4 A. Because I think it, you know, was just</p> <p>5 the start of the process which would have</p> <p>6 continued into the relevant period.</p> <p>7 Q. Okay. So you would agree that in</p> <p>8 assessing the cybersecurity practices of a</p> <p>9 company, it is acceptable to review and rely on</p> <p>10 chat messages between employees regarding those</p> <p>11 practices, right?</p> <p>12 MR. TURNER: Objection to form.</p> <p>13 I think he's relying on what's</p> <p>14 depicted in the chat message.</p> <p>15 MR. CARNEY: Okay. Speaking</p> <p>16 objection, that's completely improper.</p> <p>17 MR. TURNER: I'm just clarifying the</p> <p>18 objection. It was objection to</p> <p>19 mischaracterization of testimony.</p> <p>20 MR. CARNEY: How did I</p> <p>21 mischaracterizes it? He relied on the chat.</p> <p>22 MR. TURNER: He's relying on the</p> <p>23 screenshot that's in the chat.</p> <p>24 MR. CARNEY: Which is part of the</p> <p>25 chat, so your speaking objection --</p> <p style="text-align: center;">184</p>

<p>1 MR. TURNER: You're speaking now. I'm 2 trying to just clarify. If you left it there, I 3 wouldn't have to keep speaking. 4 MR. CARNEY: Okay. You're coaching 5 the witness during a deposition. 6 MR. TURNER: Go ahead, Chris. 7 MR. CARNEY: It's improper. I don't 8 like it. It's against the Federal Rules of Civil 9 Procedure. 10 MR. TURNER: Chris, I made a very 11 short description about the form that I was 12 objecting to. 13 Please continue. 14 MR. CARNEY: All right. 15 BY MR. CARNEY: 16 Q. Doctor, so would you agree that in 17 assessing the cybersecurity practices of a 18 company, it is acceptable to review and rely on 19 chats messages between employees regarding those 20 practices? 21 A. You know, the set of evidence I relied 22 upon, you know, in this case, you know, looked at 23 a chat that showed, you know, direct evidence of 24 the -- you know, password -- you know, how active 25 directory, you know, was -- was utilized, right?</p> <p style="text-align: center;">185</p>	<p>1 You know, in this case, it was useful 2 to show that that had been in place, because it 3 was -- there's a whole evidentiary basis to say 4 they were increasing the use of active directory. 5 Q. If I can ask you, sir, to look at 6 page 87, paragraph 158. 7 A. Page 87. 8 Q. Yes. Thank you. In the last sort of 9 clause of that paragraph, you state that there's 10 evidence establishing that, "SolarWinds generally 11 implemented password controls in a manner 12 consistent with the representations in the 13 security statement." 14 Do you see that? 15 A. Again, I'm going to read all of 158, 16 and then -- yeah, I'll answer the -- I'll ask you 17 to repeat the question, and I'll answer. 18 Q. Okay. 19 (Pause for reading/reviewing.) 20 A. Okay. 21 Q. And my question was about the 22 statement that "SolarWinds generally implemented 23 password controls in a manner consistent with the 24 representations in the security statement." 25 Do you see that?</p> <p style="text-align: center;">187</p>
<p>1 So, you know, the evidence is that, 2 you know, active directory in the following 3 paragraph discussing how Microsoft guidance around 4 password complexity. You know, in my case, that's 5 the evidence I was relying upon. 6 Q. Okay. And as you indicated, it was 7 from quite a bit outside the relevant period, 8 right? 9 A. Right. The point there being they put 10 this in place early as they were -- you know, as 11 testified in multiple places, you know, 12 increasingly using active directory so that active 13 directory, you know, was increasingly the -- the 14 source of implementation of password complexity. 15 Q. Okay. And you would then also agree 16 that in assessing the cybersecurity practices of a 17 company, it is permissible to look at documents 18 from outside the relevant period you're studying, 19 right? 20 A. In the case of showing that things 21 were in place earlier that had every -- you know, 22 reason to believe were continued and in this case 23 testimony that says active directory was the 24 primary place at which SolarWinds was seeking 25 to -- you know, manage identity.</p> <p style="text-align: center;">186</p>	<p>1 A. I do. 2 Q. And what did you mean by the word 3 "generally" in that sentence? 4 A. You know, as we've been discussing 5 throughout the day, you know, my task was to look 6 at the security statement and, you know, examine 7 whether the things in the security statement were, 8 you know -- there was -- you know, the presence of 9 process and procedure and implementation. 10 And I saw that consistent with the 11 representations in the security statement. 12 Q. All right. If I could ask you to look 13 at -- hopefully you still have in front of you 14 Exhibit 5, the securities statement. 15 A. [Speaking sotto voce]. Got it. 16 Q. On the second-to-last page with the 17 actual text on it, the page ending in 337108. 18 A. Yes. 19 Q. And under "Access Controls" and then 20 under "Authentication/Authorization," do you see 21 the sentence that says, "Our password best 22 practices enforce the use of complex passwords 23 that include both alpha and numeric characters 24 which are deployed to protect against unauthorized 25 use of the password."</p> <p style="text-align: center;">188</p>

Gregory Rattray
2/12/2025

1 Do you see that?
2 **A.** Yes, I do.
3 **Q.** And you'd agree that this assertion
4 does not include the word "generally," right?
5 **A.** The word "generally" is not in the
6 sentence you just read.
7 **Q.** And do you agree that the statement
8 would be different if it included the word
9 "generally" in it?
10 **MR. TURNER:** Objection to form.
11 **THE WITNESS:** Different -- different
12 how?
13 **BY MR. CARNEY:**
14 **Q.** Would it have a different meaning if
15 that same sentence I just read had the word
16 "generally" in it?
17 **MR. TURNER:** Object to form.
18 **THE WITNESS:** I'm not sure in the
19 context of the securities statement that's even
20 true. I don't necessarily agree with that
21 assertion.
22 **BY MR. CARNEY:**
23 **Q.** Why is that not true?
24 **A.** Because the securities statement is,
25 you know, a document that is, you know, depicting

189

1 to, you know, the vendor management people who
2 read it is the narrow -- you know, the purpose for
3 this securities statement.
4 And, you know, all -- all it's meant
5 to do is, you know, illuminate that SolarWinds
6 understood the types of controls that they had and
7 that they were -- there were practices in place.
8 So, you know, whether you said
9 generally we do that, because no one's holding
10 this to a bar of perfection, or we are -- our
11 parts were practices -- you know, in terms of the
12 use of this statement, I'm not sure it does make
13 any difference.
14 **Q.** If I could turn you back now to
15 paragraph 65 of Exhibit 1. I'll give you a page
16 number.
17 **A.** Okay.
18 **Q.** Page 33.
19 **A.** Uh-huh.
20 **Q.** You state that --
21 **A.** Oh --
22 **Q.** I'm sorry. Paragraph 65 --
23 **A.** -- I did it again.
24 **Q.** -- paragraph 33.
25 **A.** Yeah, I'm there.

190

1 **Q.** All right. And you can -- I'm going
2 to ask my question. You can have as much time as
3 you want to read for context.
4 But you say, "Given this context, my
5 understanding of the securities statement's
6 representation that SolarWinds's best practices
7 were to enforce the use of complex passwords is
8 that SolarWinds's automatically enforced password
9 complexity through technical measures where it was
10 feasible to do so."
11 Do you see that?
12 **A.** I do. I'm going to take a moment just
13 to make sure I read the, you know, entire
14 paragraph so that I understand, you know, the
15 full -- the full context.
16 (Pause for reading/reviewing.)
17 **A.** Okay.
18 **Q.** Okay. Regarding that first sentence
19 that I just read in paragraph 65 where it ends
20 with, "Where it was feasible to do so," do you
21 agree that the securities statement does not
22 include the phrase "where it is feasible to do
23 so"?
24 **A.** That --
25 **Q.** With respect to passwords?

191

1 **A.** Right. I'm just trying to -- I'm just
2 reorienting myself to that sentence.
3 The sentence, you know, doesn't need
4 to, you know, say "as feasible to do so," you
5 know, in the sense that you can't do things that
6 aren't feasible. It doesn't -- so, therefore, the
7 wording's unnecessary, but it's not there.
8 **Q.** So what would it mean for it to be not
9 feasible to do so?
10 **A.** You know, in terms of, you know,
11 enforcement of password complexity, you know, it
12 needs to be done through technical measures, you
13 know, in order to -- to, you know, automatically
14 enforce as, you know, that sentence you read said,
15 you know.
16 Therefore, you know, because you would
17 need the technology in place to automatically
18 enforce, which is the best -- which is the best
19 practice being referenced here, again, that's --
20 you know, that's why the language about not -- you
21 know, the language is missing related to
22 feasibility, because it's unnecessary.
23 **Q.** Okay. And if I could ask you to look
24 at the securities statement again --
25 **A.** Uh-huh.

192

Gregory Rattray
2/12/2025

<p>1 Q. -- you should have it in front of you, 2 that same page we were looking at. 3 A. Right. 4 Q. And in that same paragraph under 5 "Authentication/Authorization," it states, "Our 6 password policy covers all applicable information 7 systems, applications and databases." 8 Do you see that? 9 A. I do. 10 Q. And what does that mean to you? 11 A. That means there are written, you 12 know, guidance to the -- the company, you know, is 13 applicable to all -- applicable -- you know, 14 all applicable to information systems, 15 applications and databases. 16 Q. And, once again, you would agree it 17 doesn't say "where feasible to do so," right? 18 MR. TURNER: Objection to form. 19 THE WITNESS: Yeah. Correct. That 20 sentence doesn't have the clause that says, "where 21 feasible to do so." 22 BY MR. CARNEY: 23 Q. And is it fair to say that you're 24 reading that into the securities statement? 25 MR. TURNER: Objection to form.</p> <p style="text-align: center;">193</p>	<p>1 management team that there was -- you know, where 2 feasible, the -- you know, again, you don't need 3 to -- didn't need to say it. I added it to the -- 4 to paragraph 65. 5 But, you know, that for enforcement, 6 you need automation, and that -- you know, that 7 was how they enforced password best practices 8 where it was feasible. 9 BY MR. CARNEY: 10 Q. Okay. And just to address my friend 11 Mr. Turner's objection. 12 Does the "where it's feasible" concept 13 apply to the sentence that says, "Our password 14 policy covers all applicable information systems, 15 applications and databases"? 16 A. No. Because the two sentences are 17 pretty distinct, and they're -- you know, what 18 they're trying to articulate. That, you know, 19 they're -- the overall password policy, you know, 20 is -- is a general obligation, you know, across 21 those applicable information systems, applications 22 and databases. 23 The best practices language, you know, 24 necessarily is about enforcement. And you can 25 enforce where it's feasible to do so.</p> <p style="text-align: center;">195</p>
<p>1 Objection to the characterization of 2 the report and the testimony. 3 THE WITNESS: Okay. That's -- repeat 4 the question again, please. 5 BY MR. CARNEY: 6 Q. When you state in paragraph 65 that 7 you understand the security statement's 8 representation that SolarWinds's best practices 9 were to enforce the use of complex passwords, that 10 that means that SolarWinds automatically enforced 11 password complexity through technical measures 12 where it was feasible to do so, you're reading the 13 phrase "feasible to do so" into that paragraph of 14 the securities statement, right? 15 MR. TURNER: Objection to form to that 16 sentence. 17 THE WITNESS: You know, as, you know, 18 the paragraph goes on to state, you know, their 19 user access process narrative, you know, talks 20 about the fact that, you know, the use of active 21 directory as a, you know, automated means of 22 password complexity through technical measures, it 23 was the focus here. 24 And I think the securities statement 25 is just noting for a potential, you know, vendor</p> <p style="text-align: center;">194</p>	<p>1 So the -- as written in paragraph 65, 2 the feasible -- you know, the "where feasible to 3 do so" language applies to the best practices were 4 used to enforce complex passwords. 5 Q. And you mentioned just a little while 6 ago vendor management, and I think -- you can 7 correct me if I'm wrong, but the securities 8 statement was addressed towards vendor management; 9 is that right? 10 A. Yeah, that's my understanding. 11 Q. And what does "vendor management" mean 12 to you? 13 A. To me, you know, vendor management 14 teams are teams that are assessing, you know, a 15 supplier. 16 In this case, SolarWinds is a supplier 17 of products. And, you know, among many things 18 they do, one of the things they do is look at, you 19 know, those organizations. 20 And, you know, do they have the proper 21 security in place, is the risk -- you know, what 22 sort of risk does that product pose? 23 So my understanding is that origins of 24 this security statement were meant to provide, you 25 know, those type of teams an understanding of what</p> <p style="text-align: center;">196</p>

<p>1 SolarWinds's practices were.</p> <p>2 Q. So in your use of the word "vendor,"</p> <p>3 SolarWinds would be the vendor?</p> <p>4 A. Right.</p> <p>5 Q. Okay.</p> <p>6 A. The team -- just to be -- just as a</p> <p>7 clarification, the vendor management teams would</p> <p>8 be talking about would be diligencing or looking</p> <p>9 at SolarWinds and potentially the securities</p> <p>10 statement, because, yeah, SolarWinds was selling</p> <p>11 something, and the vendor management team was</p> <p>12 looking at SolarWinds.</p> <p>13 Q. All right. Sir, I'm going to ask you</p> <p>14 to turn to -- let me give you a page number --</p> <p>15 page 45 --</p> <p>16 A. Uh-huh.</p> <p>17 Q. -- paragraph 83.</p> <p>18 A. Yep.</p> <p>19 Q. And it's -- it's in the section where</p> <p>20 you're talking about software development --</p> <p>21 A. Uh-huh --</p> <p>22 Q. -- do you see that?</p> <p>23 A. -- yep.</p> <p>24 Q. And you touched on a little bit your</p> <p>25 involvement in overseeing the software development</p> <p style="text-align: center;">197</p>	<p>1 Process' created in 2016 and last updated on</p> <p>2 June 22, 2018, focused on how security testing was</p> <p>3 integrated into the process."</p> <p>4 Do you see that?</p> <p>5 A. I do. Once more, I just think it's</p> <p>6 easier for us, can I review that paragraph 90 --</p> <p>7 Q. Sure.</p> <p>8 A. -- and just make sure I got -- I got</p> <p>9 the full context -- for this.</p> <p>10 (Pause for reading/reviewing.)</p> <p>11 A. Okay. Let's proceed.</p> <p>12 Q. Okay. So in the sentences that I</p> <p>13 read, first of all, there's a Footnote 106 and you</p> <p>14 refer to a document as a -- and you can read</p> <p>15 Footnote 106, but as a "slide deck from 2015</p> <p>16 explaining basics of Agile process, including the</p> <p>17 bug 'scrub' done during each sprint."</p> <p>18 Do you see that?</p> <p>19 A. Uh-huh.</p> <p>20 Q. And here we can...</p> <p>21 (Whereupon, Exhibit 11 is marked for</p> <p>22 identification.)</p> <p>23 BY MR. CARNEY:</p> <p>24 Q. And just for the record, I've handed</p> <p>25 you what's been marked as Exhibit 11. And this is</p> <p style="text-align: center;">199</p>
<p>1 lifecycle at JPMorgan.</p> <p>2 Do you recall that?</p> <p>3 A. Yeah, it was one of the places where I</p> <p>4 was involved with that security aspects of</p> <p>5 software development, yes.</p> <p>6 Q. And did JPMorgan follow a waterfall or</p> <p>7 an Agile process?</p> <p>8 A. You know, during -- during the period</p> <p>9 I was there, there were actually -- you know, it</p> <p>10 was a large organization, and at -- they were</p> <p>11 moving towards an Agile process in some software</p> <p>12 development.</p> <p>13 I would imagine, you know, that some</p> <p>14 of it was still developed by a waterfall, very</p> <p>15 contextually -- you know, contextual.</p> <p>16 Q. Okay. So if we flip forward a few</p> <p>17 pages to paragraph 90 on page 49, you state in the</p> <p>18 middle of that paragraph, "I have reviewed various</p> <p>19 guidance documents from Confluence" -- and that's</p> <p>20 with a capital C --</p> <p>21 A. Uh-huh.</p> <p>22 Q. -- "that indicate SolarWinds followed</p> <p>23 an Agile development process."</p> <p>24 And you say, "In particular, I've</p> <p>25 reviewed a document titled 'Security Testing</p> <p style="text-align: center;">198</p>	<p>1 the presentation you reference in Footnote 106 and</p> <p>2 begins with Bates number SW-SEC-SDNY_00184276.</p> <p>3 A. That's right. And if you don't mind,</p> <p>4 I'd like to just take a moment and --</p> <p>5 Q. Sure.</p> <p>6 A. -- look through the full presentation</p> <p>7 as we go forward.</p> <p>8 (Pause for reading/reviewing.)</p> <p>9 A. Okay.</p> <p>10 Q. So, sir, just my question: Why did</p> <p>11 you rely on a slide deck from 2015 for your</p> <p>12 understanding as to SDL practices SolarWinds was</p> <p>13 following in what you defined as the relevant</p> <p>14 period of October 2018 to January of 2021?</p> <p>15 A. You know, similar to the other</p> <p>16 discussion we had, you know -- I -- you know, if</p> <p>17 you look at the full set of evidence, including,</p> <p>18 you know, Mr. Colquitt's deposition, he -- he was</p> <p>19 building on this foundation, right?</p> <p>20 So, you know, using this foundation</p> <p>21 where they were, you know -- you know, this deck</p> <p>22 is pretty foundational in terms of, you know, how</p> <p>23 to do Agile. This was a foundation that they --</p> <p>24 they built upon.</p> <p>25 So this was -- you know, the document</p> <p style="text-align: center;">200</p>

<p>1 really, you know, got to the point that: A, they 2 were using Agile, and, B, the security testing 3 process was part of how they did Agile. You know, 4 it was the best illustration of that. 5 Q. And if we turn to the third page of 6 this document -- 7 A. Uh-huh. 8 Q. -- ending in 276, do you see there's 9 a -- there's an agenda on there? 10 A. Are we talking about the contents 11 page? 12 Q. Yeah, the contents page. 13 A. Right. 14 Q. Exactly. 15 A. Yeah. 16 Q. With time allotments -- 17 A. Uh-huh. 18 Q. -- including for a break? 19 A. Right. 20 Q. Is it your understanding that this was 21 part of a presentation? 22 A. You know, I don't -- it does appear to 23 be part of a presentation -- or not part of a 24 presentation. It looks like a deck that is meant 25 to be presented --</p> <p style="text-align: center;">201</p>	<p>1 BY MR. CARNEY: 2 Q. Okay. In paragraph 94 on page 52, 3 you -- I'll let you get to that. 4 A. Okay. Yes. I'm going to read the 5 paragraph about the final security reviews. 6 (Pause for reading/reviewing.) 7 A. Okay. Yeah. 8 Q. Okay. In that paragraph 94, you 9 describe final security reviews or FSRs as "the 10 most significant artifacts I've reviewed from 11 SolarWinds's software development process." 12 So let me ask you: Why are these the 13 most significant artifacts? 14 A. Well, you know, again -- or this is in 15 the context of the more general discussion of, you 16 know, the software development lifecycle and the 17 security aspects of it. 18 So, you know, the most significant, 19 you know, related to the fact that, you know, 20 these were -- these final security reviews 21 demonstrated, you know, both, you know, deep 22 process related to, you know, how they approached, 23 you know, secure development. 24 As -- you know, as well as, you know, 25 lots of -- lots of the supporting evidence for</p> <p style="text-align: center;">203</p>
<p>1 Q. Okay. 2 A. -- you know, which is maybe a 3 different answer. 4 Q. And do you know who it was presented 5 to? 6 A. You know, this is, you know, pretty 7 clearly a deck that is meant to be presented to 8 technologists related to the development process. 9 Q. And so would you agree that in some 10 instances, it's appropriate to review slide decks 11 to gain an understanding of the cybersecurity 12 practices that a company is following? 13 MR. TURNER: Objection to form. 14 THE WITNESS: You know, there -- you 15 know, this slide deck, you know, was used to 16 evidence that SolarWinds had, you know, moved to 17 the Agile process and that security was present. 18 It was, you know, it was part of the 19 full set of evidence along with Mr. Colquitt's 20 depositions and other technology leaders about how 21 they implemented the Agile process and the 22 security processes associated with it. 23 You know, it's an element of the 24 evidence I examined. 25 ///</p> <p style="text-align: center;">202</p>	<p>1 other elements of the -- you know, the 2 implementation of evidence in addition to the 3 other sources of evidence that exist for the 4 implementation of things like testing processes. 5 Q. Okay. In paragraph 95, you talked 6 about -- that you reviewed a sample from 7 approximately 100 FSRs you received. 8 Do you see that? 9 A. That's right. 10 Q. And who selected the samples that you 11 looked at? 12 A. You know, it was similar to the 13 other -- I call these evidence tranches. I may 14 have said that before. I think we were talking 15 about the SARFs, but maybe others as well. 16 I requested, you know, evidence from 17 the Latham team of, you know, implementation -- 18 you know, implementation including things like, 19 you know, the outputs of implementation processes 20 like final security reviews. 21 So they selected -- they selected the 22 hundred. 23 Q. And then you selected the -- I'm going 24 to -- I think I counted 14-or-so samples that are 25 identified in Footnote 120?</p> <p style="text-align: center;">204</p>

Gregory Rattray
2/12/2025

<p>1 A. Right. Similar process. I looked -- 2 in this case, I know I looked at more than 50, 3 but, again, that 50 to 70 in this case as well. 4 And then I selected the subset that 5 I've cited in the report. 6 (Whereupon, Exhibit 12 is marked for 7 identification.) 8 BY MR. CARNEY: 9 Q. Okay. Dr. Rattray, I've handed you 10 what's been marked as Exhibit 12. And, for the 11 record, this is just the first sample that you 12 identify in Footnote 120 of the FSR, and it starts 13 with the Bates stamp SW-SEC-SDNY_00055119. 14 And could you just help me, just walk 15 me through this FSR, tell me what it shows. 16 A. I'm gonna just read it through myself 17 real quick -- 18 Q. Sure. 19 A. -- and then, you know, I'll walk you 20 through it. 21 Q. Thank you. 22 (Pause for reading/reviewing.) 23 A. I looked through it. 24 How should we proceed? Do you want to 25 ask the question again and, you know, give me some</p> <p style="text-align: center;">205</p>	<p>1 development process from a security perspective, 2 you know, so that the teams that are, you know, 3 working on a given product or application, you 4 know, are guided -- you know, guided in this 5 fashion. 6 So, again, it has requirements 7 analysis. Again, as we talked about things like 8 threat -- threat modeling, you know, understanding 9 security requirements are part of the element of 10 things like threat modeling. 11 It talks to the type of testing 12 outlined in the security statement. It even 13 requires scheduling of testing early. Shows 14 test -- testing results of a variety of sorts, you 15 know, all the phases outlined in the security 16 statement, you know, mapped here including to the 17 sort of product security review. 18 You know, this is the -- this is a -- 19 a process that constitutes product security 20 review, you know, shows -- shows that the 21 appropriate players were involved in the -- you 22 know, the review -- an approval phase, phase 4. 23 Q. So you mentioned that it shows testing 24 results of a variety of sorts. 25 Is it -- does this Exhibit 12 do that?</p> <p style="text-align: center;">207</p>
<p>1 parameters for the walkthrough? 2 Q. Yeah. How about I'll just ask you, to 3 speed things up. 4 Can you just tell me how documents 5 like this FSR establish to you that, if it does 6 establish that to you, that SolarWinds followed 7 all aspects of the SDL in its securities 8 statement? 9 A. Again, the FSRs were an element of the 10 determinations I made around, you know, 11 SolarWinds's, you know, software development and, 12 you know, the statements made in the securities 13 statement. 14 You know, the presence of this review 15 as process and the type of, you know, 16 implementation that we see in these reviews, you 17 know, is a pretty strong, you know -- you know, 18 not pretty. 19 It's a very strong, you know, capstone 20 on a -- on a set of the processes outlined in the 21 securities statement. 22 You know, it includes things like 23 requirements analysis, back to our -- you know, 24 its phase, there's a template, there's a series of 25 things with structure that guide the -- the</p> <p style="text-align: center;">206</p>	<p>1 Does it show test results? 2 A. I see checkmarks reports specifically 3 as test results. 4 Q. What page are you on? 5 A. I'm on the second page. 6 MR. TURNER: For the record, it's on 7 all four pages. 8 THE WITNESS: Oh, yeah. Fair enough. 9 Second page, third page -- 10 MR. TURNER: From the first as well. 11 THE WITNESS: -- and the last page. 12 Yeah, yeah, bottom of the first page. 13 BY MR. CARNEY: 14 Q. And there are -- so are you saying 15 that there are test results in this document, or 16 that it links to other documents that purport to 17 contain test results? 18 A. No. There's test results in this 19 document. The checkmark report and the data 20 there, you know, high, medium, low, you know, as 21 stated in basically all pages are test results. 22 Q. So just for the record, the results 23 themselves are in this document? 24 MR. TURNER: Just object to form. 25 Go ahead.</p> <p style="text-align: center;">208</p>

Gregory Rattray
2/12/2025

1 THE WITNESS: Yeah, it's a question of
2 what you consider results. But, you know, the --
3 the results summary in terms of high, medium and
4 low are -- you know, the test results are
5 summarized here, you know, in a few places as
6 checkmark report and I believe -- yeah, dates are
7 given.

8 And it looks like there's a link to
9 the PDF where the more detail, you know, report
10 would be available.

11 BY MR. CARNEY:

12 Q. And did you look at that more detailed
13 report?

14 A. I looked at a large number of testing
15 reports including checkmarks report.

16 Q. Did you look at the testing reports
17 associated with the samples that you have in
18 Footnote 120?

19 A. No. Similar to the other sets of
20 data, I was looking for the existence of the right
21 process and clear evidence of its implementation.

22 You know, in the case of the security
23 reviews, I've been looking at testing reports,
24 again, just to, you know, know or confirm that,
25 you know -- that the checkmark -- you know, the

209

1 types of things that were in their checkmark
2 reports, how those reports were organized, there
3 was absolutely no reason for me to believe if they
4 listed a checkmark report in any FSR, it
5 wouldn't -- you know, it wouldn't be there.

6 It would be a lot of work, you know,
7 to create summaries of results from reports that
8 didn't exist. I felt no need to look at the
9 specific reports when it was very clear that the
10 testing was, you know, going on.

11 Q. Okay. And in that same paragraph, the
12 last sentence, you said that, "The FSRs included
13 sections for engineers to post links to tickets,"
14 and in parentheses, you have, "(stories) in JIRA
15 concerning security issues found and addressed
16 through security testing, as well as places to
17 post summaries of or links to results with
18 vulnerability scans and penetration tests."

19 Can you show me where in this
20 Exhibit 12 are the sections for the engineers to
21 post links to tickets concerning security issues
22 found?

23 MR. TURNER: I have to object here.
24 Because this issue is noted in
25 Footnote 120. I want to make sure you've seen

210

1 that.

2 The problem is these can't be printed
3 today with the links live, but the linked
4 documents were produced separately and covered in
5 the footnote.

6 BY MR. CARNEY:

7 Q. Okay. And to counsel's whatever that
8 was, did you look at the linked documents?

9 A. There was a set of linked documents
10 produced, and I did look at those.

11 Q. And did you look at the linked
12 documents for the samples that you selected in
13 Footnote 120?

14 A. The -- you know, the -- you know,
15 looked at a produced set of links. Again, you
16 know, in the process of producing, you know, the
17 material, you know, both for the security review
18 and the presence of supporting, you know, JIRA --
19 JIRA-based documentation, as -- it was just
20 described, you know, that turned out to be not at
21 the same time.

22 So I didn't have the FSRs with the --
23 I'm sorry, had the JIRA tickets associated with an
24 FSR in sort of a single production.

25 You know, I made an effort to -- you

211

1 know, when I went through the JIRA reports to, you
2 know, look at, you know, as process, the types of
3 things they linked back to.

4 I did not map every, you know -- every
5 FSR to the JIRA reports that I was looking at,
6 because as we've been discussing today, that sort
7 of analysis was well below the level necessary to
8 sort of understand that the securities statements,
9 you know -- you know, illumination.

10 Or when the security statement said
11 there was a secure development process -- you
12 know, set of activities, you know, such as testing
13 activities, the final security reviews provided,
14 you know, strong evidence of that, you know, that
15 I saw that were linked to issue identification.

16 I saw tickets that indicated that
17 that -- you know, that -- those JIRA links did
18 exist, right? They were broken in some of the FSR
19 documentation.

20 And that this robust process was, you
21 know, being executed and, you know, met -- you
22 know, met what I needed in terms of how the
23 industry would approach validating that the things
24 in the security statement, you know, such as pen
25 testing and static testing were in place.

212

<p>1 Q. Sir, if I could ask you to turn to 2 paragraph 101 of Exhibit 1.</p> <p>3 A. Uh-huh.</p> <p>4 Q. And this is on page 56.</p> <p>5 And you're discussing what you 6 perceived to be problems with Mr. Graff's 7 methodology, right?</p> <p>8 A. Yeah, I should, again --</p> <p>9 Q. Okay.</p> <p>10 A. -- read these as you start to ask 11 questions. Is that -- I shouldn't assume that's 12 fine.</p> <p>13 Q. Of course. Of course. 14 (Pause for reading/reviewing.)</p> <p>15 A. Okay.</p> <p>16 Q. In paragraph 101, maybe it's the 17 fourth sentence down, you say, "Cybersecurity 18 assessments generally do not involve reviewing 19 employees' emails or presentations to management 20 in the first place."</p> <p>21 And then parenthesis, "(let alone 22 stray comments or notations in such documents that 23 lack appropriate context)."</p> <p>24 Do you see that?</p> <p>25 A. Right.</p> <p style="text-align: center;">213</p>	<p>1 practices.</p> <p>2 Q. But you exercised your judgment and 3 determined that it was appropriate to look at that 4 particular presentation, right?</p> <p>5 A. Yes.</p> <p>6 Q. Okay. And with the chat we looked at 7 earlier with the screenshot, you exercised your 8 judgment and determined that it was appropriate to 9 look at that particular chat with the screenshot, 10 right?</p> <p>11 MR. TURNER: Object to form.</p> <p>12 THE WITNESS: Right. You know, the 13 sentence, you know, continues to say, "let alone 14 stray comments or notations in documents."</p> <p>15 You know, in the case of the 16 PowerPoint presentation on Agile, it was a full 17 presentation that was, again, illuminating that -- 18 this sort of foundational, you know, movement and 19 conceptualization of SolarWinds in that area.</p> <p>20 It was not a single notation inside, 21 you know -- you know, inside a presentation. It 22 was, you know -- it was a -- sort of the full 23 presentation. You know, I felt like it was -- it 24 was very useful in illustrating how -- you know, 25 how they were thinking about this, which was what</p> <p style="text-align: center;">215</p>
<p>1 Q. We looked at -- a little while ago, 2 you relied on a presentation that documented what 3 you thought was the company's SDL process, right?</p> <p>4 MR. TURNER: Object to form.</p> <p>5 THE WITNESS: If we're talking about 6 the presentation about Agile -- right? -- you 7 know, it included, you know -- it included how 8 Agile is conducted and then security steps during 9 Agile development.</p> <p>10 BY MR. CARNEY:</p> <p>11 Q. Okay. And you made an assessment 12 using your cybersecurity experience that it was 13 appropriate to rely on that presentation from 2015 14 to -- in forming your opinions, right?</p> <p>15 A. That was an element of, you know, what 16 I looked at. You know, I looked at, you know, 17 unlike Mr. Graff, you know, the policies, a very 18 large set of documentary evidence, you know, 19 process, things like FSRs.</p> <p>20 I used that document because it was a 21 good baseline, as we said, about what they were -- 22 you know, how they understood that process of 23 Agile and where a security fit into it, but it was 24 not the base -- you know, the sole basis of my, 25 you know, assessment of their secure development</p> <p style="text-align: center;">214</p>	<p>1 I was trying to do there.</p> <p>2 You know, as we discussed in the case 3 of the email, it was, you know, documenting 4 Microsoft's, you know, process. It was contained 5 within an email, but the point was active 6 directory, you know, had strong -- the ability to 7 implement strong -- strong passwords.</p> <p>8 So it wasn't an opinion. It wasn't a 9 comment. It was, you know, linkage to a global 10 technologies company's, you know, product and its 11 features regarding strong passwords.</p> <p>12 BY MR. CARNEY:</p> <p>13 Q. Okay. Let me ask you, please, to turn 14 to paragraph 121. And this is on page 67.</p> <p>15 A. Uh-huh.</p> <p>16 Q. And I'll just let you know that 17 paragraphs 121 through 126, you discuss this issue 18 of developer access to billing data for test 19 purposes.</p> <p>20 And you can look -- as we go along, 21 you can look --</p> <p>22 A. Uh-huh.</p> <p>23 Q. -- at as much of it as you want to get 24 context. But I'm gonna hand you the email 25 that's -- that you're discussing.</p> <p style="text-align: center;">216</p>

Gregory Rattray
2/12/2025

<p>1 A. Okay. 2 (Whereupon, Exhibit 13 is marked for 3 identification.) 4 THE WITNESS: I'm going to take a 5 quick moment and, you know, just read the material 6 and the statement related to this situation. 7 BY MR. CARNEY: 8 Q. Okay. 9 (Pause for reading/reviewing.) 10 A. I just want to familiarize, you 11 know... 12 Yep. I'm ready. 13 Q. Great. 14 So you've been handed what's been 15 marked as Exhibit 13 -- 16 A. Uh-huh. 17 Q. -- and this is an email chain that you 18 reference in Footnote 160 of your report, and it's 19 Bates stamped SW-SEC-00254254. 20 A. Understood. 21 Q. All right. So if we could -- I just 22 want to see if we can agree on some things. 23 If we go to the second-to-last page of 24 this document -- 25 A. Uh-huh.</p> <p style="text-align: center;">217</p>	<p>1 BY MR. CARNEY: 2 Q. Great. And that's -- 3 A. Okay. 4 Q. -- all I was asking. Thank you. 5 And based on your cybersecurity 6 experience, why is that a security incident? 7 MR. TURNER: Object to form. 8 THE STENOGRAPHER: Excuse me. I 9 couldn't hear you. 10 MR. TURNER: And the term "incident." 11 THE WITNESS: The sharing of -- this 12 is a -- you know, are we talking about this 13 specific situation or just generally password 14 sharing? 15 BY MR. CARNEY: 16 Q. Well, you had said in your prior 17 response that a fact that a different SolarWinds 18 employee using a password is a security incident, 19 and I'm just trying to understand why it was a 20 security incident. 21 A. You know, again, just sort of 22 generally password sharing, you know, is not seen 23 as something that should occur, and, you know, 24 security policies, you know, user -- you know, 25 user access policies where people are told about</p> <p style="text-align: center;">219</p>
<p>1 Q. -- which is -- ends in 265. 2 A. Okay. 3 Q. And if we look at that email -- 4 because these threads are obviously in reverse 5 chronological order. 6 A. Yep. 7 Q. If we look at that email at the bottom 8 from Sean O'Shea, it says in the first bullet, 9 "They're currently using a shared login currently 10 of a different SolarWinds employee. This is 11 definitely a security incident and needs to stop." 12 Do you agree with that sentiment, that 13 this was definitely a security incident that 14 needed to stop? 15 MR. TURNER: Objection to form. 16 Foundation. 17 THE WITNESS: You know, the -- the 18 identification of this is an incident and, you 19 know -- and I'm also aware that they did, you 20 know -- yeah, they -- they treated this, you know, 21 with a lot of, you know, attention. 22 So I guess -- if the question is: 23 Is -- you know, is the fact that a different 24 SolarWinds employee using a password as a security 25 incident, yes.</p> <p style="text-align: center;">218</p>	<p>1 what -- how they should use their -- use their 2 access, you know, you generally don't -- you know, 3 generally say you should not do that. 4 Q. Okay. And would sharing login 5 information violate any of the tenets of the 6 SolarWinds's public-facing security statement? 7 A. No, it would not. 8 Q. And why do you say that? 9 A. Because, you know, the -- you know, 10 when I -- as we read the security statement, 11 there's no specific prohibition about password 12 sharing. 13 Q. So if I could ask you to look back at 14 the security statement, Exhibit 5. 15 A. Uh-huh. 16 Q. You have that in front of you? 17 A. Yes. 18 Q. Okay. And the page ending in 337108. 19 Do you see that? 20 A. Yes, I do. 21 Q. And under "Authentication and 22 Authorization," the first sentence says, "We 23 require that authorized users be provisioned with 24 unique account IDs." 25 Do you see that?</p> <p style="text-align: center;">220</p>

Gregory Rattray
2/12/2025

<p>1 A. I do.</p> <p>2 Q. In your mind, does that statement</p> <p>3 prohibit the sharing of login information between</p> <p>4 employees?</p> <p>5 A. No.</p> <p>6 Q. And why not?</p> <p>7 A. Because, I mean, it's talking about</p> <p>8 provisioning, not how people use their IDs.</p> <p>9 Q. And just so I'm clear, nothing in</p> <p>10 SolarWinds's security statement precludes</p> <p>11 employees from sharing their logins and passwords</p> <p>12 with each other?</p> <p>13 A. You know, as we just discussed, the</p> <p>14 fact that authorized users are provisioned with</p> <p>15 unique account IDs is what the security statement</p> <p>16 says, and there's nothing in there -- nothing in</p> <p>17 the security statement about shared passwords.</p> <p>18 Q. All right. In the email above in the</p> <p>19 thread, that same page that we're at --</p> <p>20 A. Sorry. I'm just sorting my</p> <p>21 documentation.</p> <p>22 Q. -- exhibit -- yeah, Exhibit 13.</p> <p>23 A. Yeah, I'm just trying to get the other</p> <p>24 documentation out. Okay.</p> <p>25 So we're -- I'm back to the point we</p> <p style="text-align: center;">221</p>	<p>1 But I don't -- I don't generally agree</p> <p>2 that under no circumstances is development to be</p> <p>3 done in production.</p> <p>4 BY MR. CARNEY:</p> <p>5 Q. Why do you say you don't know the</p> <p>6 context in which he was writing this email?</p> <p>7 A. I mean, he's urgently responding to</p> <p>8 this initial email. You know, he -- I think he's</p> <p>9 showing urgency around, you know, a situation</p> <p>10 which he wants to get control.</p> <p>11 You know, that's what I know about the</p> <p>12 context of this.</p> <p>13 Q. Okay. And, in fact, in your report,</p> <p>14 Exhibit 1, starting at paragraph 122 --</p> <p>15 A. Uh-huh.</p> <p>16 Q. -- don't you write several paragraphs</p> <p>17 about this particular incident that Mr. Day is</p> <p>18 discussing?</p> <p>19 A. Right. No. I have a lot of context</p> <p>20 about the incident as a whole. I think the point</p> <p>21 I'm making is any given email -- you know, I don't</p> <p>22 know what he was doing at that time of day and why</p> <p>23 he chose the language that, you know, is here,</p> <p>24 which, again, I disagree with, because, you</p> <p>25 know -- you know, there's elements of this that</p> <p style="text-align: center;">223</p>
<p>1 were at where -- like, the last email. So, yeah,</p> <p>2 I'm --</p> <p>3 Q. Okay.</p> <p>4 A. Yep.</p> <p>5 Q. And the email above --</p> <p>6 A. Uh-huh.</p> <p>7 Q. -- there's one from Chris Day.</p> <p>8 Do you see that?</p> <p>9 A. Yep.</p> <p>10 Q. And he writes, "Hello. Highlighted</p> <p>11 item needs to stop immediately. Under no</p> <p>12 circumstances is development to be done in</p> <p>13 production. If that impacts deliverables, please</p> <p>14 let August know. This is a significant security</p> <p>15 and SOX violation."</p> <p>16 Do you see that?</p> <p>17 A. I do.</p> <p>18 Q. Do you agree with Mr. Day's statement</p> <p>19 that under no circumstances is development to be</p> <p>20 done in production?</p> <p>21 MR. TURNER: Objection to form.</p> <p>22 THE WITNESS: Not necessarily. I</p> <p>23 don't -- you know, I don't know the -- I mean, the</p> <p>24 context, you know, of -- in which he was writing</p> <p>25 this email.</p> <p style="text-align: center;">222</p>	<p>1 show urgency.</p> <p>2 So I don't know what was happening to</p> <p>3 Chris Day at that time when he decided to write</p> <p>4 this email this way.</p> <p>5 Q. When Mr. Day said that "This is a</p> <p>6 significant security and SOX violation," do you</p> <p>7 agree with him?</p> <p>8 A. The notion that "significant," I don't</p> <p>9 agree with.</p> <p>10 Q. Why not?</p> <p>11 A. This was, you know, a minor incident.</p> <p>12 You know, and -- you know, as they went through</p> <p>13 the process, it was -- I'm just gonna check and</p> <p>14 make sure I got the right word, but I believe that</p> <p>15 the chief -- you know, the head of information</p> <p>16 security, Tim, you know, said he thought the risk</p> <p>17 was low.</p> <p>18 And so, you know, again, I don't think</p> <p>19 it's a significant security violation.</p> <p>20 Q. Did you ever talk to Chris Day?</p> <p>21 A. I did not.</p> <p>22 Q. Did you ask to talk to him?</p> <p>23 A. I did not.</p> <p>24 Q. What do you understand the</p> <p>25 statement -- well, first of all, let me back up a</p> <p style="text-align: center;">224</p>

Gregory Rattray
2/12/2025

<p>1 second.</p> <p>2 Do you agree that it's a SOX</p> <p>3 violation?</p> <p>4 MR. TURNER: Objection to form and</p> <p>5 foundation.</p> <p>6 THE WITNESS: You know, I don't know</p> <p>7 all the specific provisions of SOX. I know pretty</p> <p>8 deeply that the provisions that relate to</p> <p>9 information security, you know, shared passwords,</p> <p>10 may be identified as a specific SOX violation, you</p> <p>11 know, in which case, you know, that would be a</p> <p>12 violation, yes.</p> <p>13 BY MR. CARNEY:</p> <p>14 Q. Well, and just to be clear, the</p> <p>15 highlighted portion that he's referring to is the</p> <p>16 development being done in production, right?</p> <p>17 A. Right. But that doesn't necessarily</p> <p>18 mean that the violation is -- you know, is that</p> <p>19 element of what he's highlighted that Chris Day is</p> <p>20 talking about.</p> <p>21 Q. Well, and just for context, he says in</p> <p>22 his email, "Highlighted item needs to stop</p> <p>23 immediately," right?</p> <p>24 A. Yes. Because Chris's email says, "The</p> <p>25 highlighted item needs to stop immediately."</p> <p style="text-align: center;">225</p>	<p>1 like, the safety of financial controls.</p> <p>2 Q. All right. And so you -- just so</p> <p>3 we're clear, you don't think either the sharing of</p> <p>4 the passwords or the development being done in the</p> <p>5 production environment were significant security</p> <p>6 issues?</p> <p>7 A. You know, in this instance, no.</p> <p>8 MR. CARNEY: A couple more questions</p> <p>9 on this, and then we'll take a break.</p> <p>10 MR. TURNER: Thank you.</p> <p>11 THE WITNESS: Uh-huh.</p> <p>12 BY MR. CARNEY:</p> <p>13 Q. Do you agree that not sharing</p> <p>14 passwords is a cybersecurity best practice?</p> <p>15 A. Yes. Yeah.</p> <p>16 Q. Okay.</p> <p>17 A. It's a best practice, because humans</p> <p>18 tend to want to do things that are easy. And the</p> <p>19 type of practice that requires constant attention</p> <p>20 that occurs quite often, but it's not -- you know,</p> <p>21 it's not practice that we wanted to have happen in</p> <p>22 a security practice.</p> <p>23 MR. CARNEY: Okay. We can take a</p> <p>24 break now.</p> <p>25 THE WITNESS: Okay.</p> <p style="text-align: center;">227</p>
<p>1 Q. And so when he's saying, "This is a</p> <p>2 significant security and SOX violation," he's</p> <p>3 referring to development being done in production</p> <p>4 environment, right?</p> <p>5 A. Yes. It does appear --</p> <p>6 Q. Okay.</p> <p>7 A. -- so.</p> <p>8 Q. And were your earlier responses to my</p> <p>9 questions reflecting that, or were they reflecting</p> <p>10 the password sharing issue?</p> <p>11 MR. TURNER: Object to form.</p> <p>12 THE WITNESS: Yeah, well, in general,</p> <p>13 I don't agree that it was a significant security</p> <p>14 instance.</p> <p>15 I don't know which aspect of this</p> <p>16 specific minor incident he's referring to, the SOX</p> <p>17 violation, you know, you did just read that, you</p> <p>18 know, the email refers to development.</p> <p>19 May -- he may have been referring to</p> <p>20 that in terms of a SOX violation --</p> <p>21 BY MR. CARNEY:</p> <p>22 Q. Okay.</p> <p>23 A. -- which is not, you know, necessarily</p> <p>24 an information security violation, because the SOX</p> <p>25 is a -- you know, a control structure around --</p> <p style="text-align: center;">226</p>	<p>1 THE VIDEOGRAPHER: The time right now</p> <p>2 is 4:11 p.m.</p> <p>3 We are off the record.</p> <p>4 (Whereupon, a recess was taken at</p> <p>5 4:12 p.m.)</p> <p>6 THE VIDEOGRAPHER: The time right now</p> <p>7 is 4:28 p.m.</p> <p>8 We're back on the record.</p> <p>9 BY MR. CARNEY:</p> <p>10 Q. All right. Dr. Rattray, before we</p> <p>11 broke, we were looking at Exhibit 13. I just had</p> <p>12 one --</p> <p>13 A. Oh, yeah. Okay.</p> <p>14 Q. -- the email --</p> <p>15 A. Uh-huh.</p> <p>16 Q. And I just want to ask you: You had</p> <p>17 mentioned that when we were talking about Chris</p> <p>18 Day's email in particular --</p> <p>19 A. Right.</p> <p>20 Q. -- that you didn't know what was</p> <p>21 happening to him that day.</p> <p>22 What did you mean by that?</p> <p>23 A. You know, I think as I mentioned,</p> <p>24 there was a lot of urgency in this email. You</p> <p>25 know -- you know, that -- actually, I sort of see</p> <p style="text-align: center;">228</p>

Gregory Rattray
2/12/2025

<p>1 this email, you know, in a very good way in terms 2 of just overall SolarWinds security practice 3 where, you know, the technology leaders, you know, 4 over and over, again, you know, see it imperative 5 to, you know, highlight things that are 6 security -- you know, potential security issues 7 and, you know, be clear like a coach is clear in 8 practice that if you miss a block, you really 9 shouldn't do that in a game.</p> <p>10 So, you know, I don't know whether the 11 urgency in the email is him seeking to be a good 12 coach or, you know, a day where he had a lot going 13 on and, you know, wanted to get this, you know, 14 urgency delivered quickly. This is a pretty short 15 email.</p> <p>16 Q. So I understand, is it your view that 17 with most emails, you sort of need to know what 18 was going on with the person's day to be able to 19 understand them or to rely on them?</p> <p>20 A. You know, I think this is one of the 21 reasons why emails like this are not great sources 22 of assessment of security -- you know, the 23 presence of the -- you know, the practices 24 outlined in this securities statement.</p> <p>25 You do need context for emails to</p> <p style="text-align: center;">229</p>	<p>1 please turn to paragraph 212 of Exhibit 1 of your 2 expert report. And I'll get you a page number. 3 My outline just has the paragraph numbers. That's 4 why it takes me a while.</p> <p>5 A. [Speaking sotto voce]. 6 The paragraph again? I could probably 7 just go right to the paragraph.</p> <p>8 Q. It is 212, which was on page 116.</p> <p>9 A. Okay.</p> <p>10 Q. And you're discussing a document that 11 Mr. Graff cites relating to threat modeling. I 12 have the document right here if you need to see 13 it.</p> <p>14 And just -- to let you know, I'm not 15 trying to hide documents from you. I'm just 16 trying to move this along. But if you need the 17 document, I got it.</p> <p>18 A. Uh-huh.</p> <p>19 MR. TURNER: I would prefer if you. 20 (Simultaneous unreportable crosstalk 21 occurs among parties.) 22 THE WITNESS: I think that's probably 23 a good idea. 24 (Whereupon, Exhibit 14 is marked for 25 identification.)</p> <p style="text-align: center;">231</p>
<p>1 understand, you know, what -- you know, what was 2 happening, you know, in -- and it's very difficult 3 to get that context.</p> <p>4 So, you know, in typical industry 5 practice, you know, you may -- you may use, you 6 know, artifacts that are found in emails, but 7 you're really not looking at this sort of 8 chat-type email as the assessment of a presence of 9 a practice.</p> <p>10 Q. Okay. And you just -- you used an 11 analogy about missing a block during practice and 12 being told not to do it during a game.</p> <p>13 Does that -- does that apply here? 14 Was this practice that we're talking about, or was 15 this the game?</p> <p>16 A. You know, I don't think this was 17 that -- you know, was not a significant security 18 incident. You know, the ongoing, you know, 19 practice of security, you know, requires 20 encouragement, you know, in an ongoing basis, 21 right?</p> <p>22 So, you know, that was just an analogy 23 to sort of talk to why the urgency might be here. 24 I don't have the context for this statement.</p> <p>25 Q. Okay. Sir, if I could ask you to</p> <p style="text-align: center;">230</p>	<p>1 BY MR. CARNEY: 2 Q. Okay. So in paragraph 212 of your 3 report, you're discussing a document that 4 Mr. Graff cited, and in Footnote 358 of your 5 report, you cite to the document.</p> <p>6 And so what I've handed you that's 7 been marked as Exhibit 14 is that document. And, 8 for the record, it has Bates stamp 9 SW-SEC-00166790.</p> <p>10 And in the paragraph in your report, 11 you state sort of about halfway down through that 12 paragraph in 212, "The authors who wrote this 13 assessment who are not deposed may have had in 14 mind a formalized type of threat modeling that 15 they wanted to be done rather than meaning to say 16 that no type of threat modeling was being done in 17 any sense."</p> <p>18 Do you see that?</p> <p>19 A. Yes.</p> <p>20 Q. Have you seen any document indicating 21 that the people who wrote "no threat modeling or 22 analysis is performed as part of any process 23 except MSP backup engineering" meant something 24 other than no threat modeling or analysis is 25 performed as part of any process?</p> <p style="text-align: center;">232</p>

<p>1 A. That was a pretty complex question.</p> <p>2 Q. Sure.</p> <p>3 A. Can you restate --</p> <p>4 Q. Sure.</p> <p>5 A. -- it?</p> <p>6 Q. I'll break it down for you.</p> <p>7 Paragraph 212, you say that Mr. Graff</p> <p>8 cites a notation in this assessment --</p> <p>9 A. Yes.</p> <p>10 Q. -- Exhibit 14, that says no threat</p> <p>11 modeling or analysis is performed as part of any</p> <p>12 process except MSP backup engineering, right?</p> <p>13 A. Yes. I see that, yep.</p> <p>14 Q. And then you say that it's -- you go</p> <p>15 on to say, "It's unclear exactly what was meant by</p> <p>16 the remark in the document," right?</p> <p>17 A. That's right.</p> <p>18 Q. And you also go on to say that the</p> <p>19 authors who wrote this assessment, they may have</p> <p>20 had in mind a formalized type of threat modeling</p> <p>21 that they wanted to be done rather than meaning to</p> <p>22 say that no type of threat modeling was being done</p> <p>23 in any sense.</p> <p>24 I wonder, what is the basis for your</p> <p>25 statement about what they may have had in mind.</p> <p style="text-align: center;">233</p>	<p>1 might have a more formalistic view of threat</p> <p>2 modeling.</p> <p>3 Q. And what would a formalistic view of</p> <p>4 threat modeling entail?</p> <p>5 A. You know, again, because I don't --</p> <p>6 you know, I see it broadly. You know, I've seen,</p> <p>7 you know, at times detailed descriptions of threat</p> <p>8 modeling processes.</p> <p>9 You know, that maybe, again, they were</p> <p>10 looking for a checklist around, you know, the</p> <p>11 performance of threat modeling specifically or the</p> <p>12 production of specific threat modeling artifacts.</p> <p>13 Which, again, there are processes that</p> <p>14 exist that cause that to happen. But, you know,</p> <p>15 it's -- as discussed, you know, multiple times, I</p> <p>16 don't see that as sort of the general industry</p> <p>17 approach for threat modeling.</p> <p>18 It's more a broad set of activities</p> <p>19 related to identification of security risk, taking</p> <p>20 that into account as you do software development.</p> <p>21 Q. So specifically related to MSP</p> <p>22 products, which this exhibit that we were looking</p> <p>23 at is discussing Exhibit 14 --</p> <p>24 A. Uh-huh.</p> <p>25 Q. -- what, if any, documents did you</p> <p style="text-align: center;">235</p>
<p>1 A. You know, well, it starts from the</p> <p>2 discussion that we had, you know, I think at the</p> <p>3 beginning, you know, of today, which is, you know,</p> <p>4 "threat modeling" is, you know, a broad term.</p> <p>5 And, you know, as we've discussed</p> <p>6 during the course of the day, you know, I see</p> <p>7 evidence, you know, that threat modeling, you</p> <p>8 know, existed in SolarWinds's practice noting that</p> <p>9 threat modeling is not part of the securities</p> <p>10 statement.</p> <p>11 But, you know -- you know, I did sort</p> <p>12 of look at the SolarWinds practices to the extent</p> <p>13 that they, you know, evidenced threat modeling,</p> <p>14 and I find that evidence there.</p> <p>15 So because of that, you know, I was --</p> <p>16 you know, I spec -- you know, speculated that they</p> <p>17 may have a formalized view of threat modeling,</p> <p>18 because I -- what they found was in the face of</p> <p>19 what I saw related to the existence of threat</p> <p>20 modeling, you know.</p> <p>21 And I reviewed the -- the FSRs for</p> <p>22 those specific, you know, products or applications</p> <p>23 just the fact that there was an FSR is evidence of</p> <p>24 threat modeling in my mind.</p> <p>25 So that was why I thought that they</p> <p style="text-align: center;">234</p>	<p>1 review regarding threat modeling in MSP products?</p> <p>2 A. Well, you know, as stated in my</p> <p>3 report, I looked at the FSRs for the software</p> <p>4 releases for the three cited, you know, RMM,</p> <p>5 backup and N-Central.</p> <p>6 And, you know, they show that the</p> <p>7 development teams were doing threat modeling, you</p> <p>8 know, identifying risks to software and developing</p> <p>9 mitigation.</p> <p>10 So that was the documentation that I</p> <p>11 used in this specific case.</p> <p>12 Q. Okay. So let's take a look at that</p> <p>13 then.</p> <p>14 If I could ask you to turn to</p> <p>15 page 114, paragraph 210 of your report.</p> <p>16 A. Uh-huh.</p> <p>17 Q. And you state that, "I've also seen</p> <p>18 evidence of threat modeling and FSRs that I've</p> <p>19 reviewed. The FSRs have sections addressing</p> <p>20 security design considerations with such headings</p> <p>21 as proactive review of all FAS, high-level design</p> <p>22 documents, documents with security design</p> <p>23 implications for security-related features</p> <p>24 identified by teams."</p> <p>25 Do you see that?</p> <p style="text-align: center;">236</p>

Gregory Rattray
2/12/2025

<p>1 A. Yes.</p> <p>2 Q. So the first quote that you have where</p> <p>3 it says, "Proactive review of all" -- and this is</p> <p>4 in all caps, "FAS," and then parentheses,</p> <p>5 "(high-level design documents,)" you cite to --</p> <p>6 you have Footnote 346, and you cite to a document.</p> <p>7 Do you see that?</p> <p>8 A. Yes.</p> <p>9 (Whereupon, Exhibit 15 is marked for</p> <p>10 identification.)</p> <p>11 BY MR. CARNEY:</p> <p>12 Q. And just, for the record, you've been</p> <p>13 handed what's been marked as Exhibit 15. And this</p> <p>14 is the document that you cite in Footnote 346,</p> <p>15 paragraph 210, and the Bates stamp is</p> <p>16 SW-SEC-SDNY_00069825.</p> <p>17 First of all, what does -- in this</p> <p>18 sentence that I just read, "Proactive Review of</p> <p>19 All FAS High-Level Design Documents," what does</p> <p>20 FAS mean?</p> <p>21 A. I don't know. I do not know what</p> <p>22 that -- that breakdown of that acronym is.</p> <p>23 Q. And would you agree that under</p> <p>24 "Proactive Review of All FAS High-Level Feature</p> <p>25 Design Documents," which is on the first page of</p> <p style="text-align: center;">237</p>	<p>1 The point here is that this FSR</p> <p>2 process is an element of, you know, them having</p> <p>3 generally threat modeling.</p> <p>4 Q. Okay. So, first of all, this document</p> <p>5 is the one document that you cite related to</p> <p>6 proactive review of all FAS high-level design</p> <p>7 documents, right?</p> <p>8 A. Yes. This is the document.</p> <p>9 Q. Okay.</p> <p>10 A. Yeah. I cite it as showing that FSRs</p> <p>11 have headings, and the heading is in the document.</p> <p>12 Q. And so is it fair to say that you're</p> <p>13 relying on the heading on the document and not the</p> <p>14 substance of any design review that was done,</p> <p>15 right?</p> <p>16 MR. TURNER: In this particular case?</p> <p>17 MR. CARNEY: In the one example that</p> <p>18 he selected, yes.</p> <p>19 THE WITNESS: Yeah, the -- I mean, you</p> <p>20 know, the sentence is not intended to, you know,</p> <p>21 look at any of these specific FSRs as -- you know,</p> <p>22 any of these specific FSRs.</p> <p>23 It's to make the point that the</p> <p>24 process of final security reviews included design</p> <p>25 considerations, which is part of, you know, a</p> <p style="text-align: center;">239</p>
<p>1 this document --</p> <p>2 A. Uh-huh.</p> <p>3 Q. -- there's an empty table?</p> <p>4 A. You know, in this case, the table is</p> <p>5 empty. But the statement is about, you know, the</p> <p>6 fact that FSRs are asking the teams to, you know,</p> <p>7 look at, you know -- you know, design documents in</p> <p>8 light of security.</p> <p>9 The first statement of paragraph -- or</p> <p>10 sorry, yeah, the first statement of paragraph 210</p> <p>11 is to the point where -- to the point that broadly</p> <p>12 you have threat modeling is about bringing in</p> <p>13 security to design considerations.</p> <p>14 And the point being made is -- it's</p> <p>15 actually the second sentence, that the FSRs</p> <p>16 have -- are as templates have sections that are,</p> <p>17 you know, asking -- you know, the teams in terms</p> <p>18 of the security element of their, you know,</p> <p>19 software -- yeah, the security -- yeah, security</p> <p>20 element of this software development to consider</p> <p>21 things.</p> <p>22 In any given instance, it -- you know,</p> <p>23 I'm not trying to say that, you know, every FSR</p> <p>24 needs to, you know, have implementations of, you</p> <p>25 know, the headings that are in the FSR.</p> <p style="text-align: center;">238</p>	<p>1 broad conception of threat modeling, which is not</p> <p>2 even in the securities statement.</p> <p>3 BY MR. CARNEY:</p> <p>4 Q. Okay. And so -- but would you agree,</p> <p>5 that given there's an empty table here, that this</p> <p>6 particular document does not support the statement</p> <p>7 that SolarWinds's developers conducted proactive</p> <p>8 reviews of all FAS documents?</p> <p>9 MR. TURNER: Object to form.</p> <p>10 THE WITNESS: No. I mean, because the</p> <p>11 simple point being made in paragraph 210 is the</p> <p>12 FSR process, you know, included, you know,</p> <p>13 callouts to look at these things. The sentence</p> <p>14 was never to look at the -- the specific</p> <p>15 implementation against a specific, you know,</p> <p>16 app -- application.</p> <p>17 Again, it's just making the general</p> <p>18 point that they had a strong FSR process, and that</p> <p>19 that -- you know, also meant that they were -- you</p> <p>20 know, especially because of the way they</p> <p>21 implemented it, they were doing threat modeling.</p> <p>22 (Whereupon, Exhibit 16 is marked for</p> <p>23 identification.)</p> <p>24 BY MR. CARNEY:</p> <p>25 Q. All right. Doctor, I've handed you --</p> <p style="text-align: center;">240</p>

Gregory Rattray
2/12/2025

<p>1 if you look at the next sort of part of that 2 sentence, it refers to -- in paragraph 210 of 3 Exhibit 1, first to "documents with security 4 design implications," and there's a Footnote 347. 5 Do you see that? 6 A. Yes. 7 Q. Okay. And so what you've been handed 8 as Exhibit 16 is the document that is cited in 9 Footnote 347. 10 MR. CARNEY: And, for the record, 11 that's SW-SEC-SDNY_00055006. 12 BY MR. CARNEY: 13 Q. Do you -- where it says "Documents 14 With Security Design Implications or Data Privacy 15 Concerns" at the top, do you see the table 16 underneath that? 17 A. I do. 18 Q. And that table has -- appears to have 19 links to two documents? 20 A. That's correct. 21 Q. Have you been able to access either 22 the documents that these links point to? 23 A. There was no need for me to access 24 either of those documents. 25 Q. And why not?</p> <p style="text-align: center;">241</p>	<p>1 at the documents for the reasons that that was 2 unnecessary. 3 Q. Let me ask you: Outside of litigation 4 when you're assessing the cybersecurity of a 5 company, would it be your practice to rely on the 6 title of a section in a document versus looking at 7 the underlying documentation? 8 MR. TURNER: Object to form. 9 THE WITNESS: In terms of, you know -- 10 can you repeat the question? 11 BY MR. CARNEY: 12 Q. Sure. 13 I'm just -- I'm trying to understand 14 this -- you know, you talk about how Next Peak 15 does this cybersecurity -- 16 A. Uh-huh. 17 Q. -- assessments, and I'm wondering if 18 the concept of looking at a heading in a final 19 security review without looking at the underlying 20 documentation is consistent with the sort of 21 non-litigation cybersecurity assessments that you 22 perform at Next Peak? 23 MR. TURNER: Object to form. 24 THE WITNESS: That -- you know, 25 this -- we're talking about a specific sentence</p> <p style="text-align: center;">243</p>
<p>1 A. Because as we were just discussing 2 with the heading proactive review of all FAS 3 high-level design documents, that the heading 4 documents with design implications was simply to 5 illuminate that the FSRs have, as a -- as 6 templates, you know -- you know, look at, you 7 know, security as a feature in design. 8 And, you know, call out for 9 development teams, because they will go through 10 the FSR process to look for the presence of these 11 things. 12 As I said in the last conversation 13 around the proactive review of all FAS high-level 14 design documents, the intent of that sentence was 15 never to look at a specific, you know, FSR, you 16 know, as evidence of implementation of, you know, 17 threat modeling. 18 It was to show that the FSR process 19 hit the things that threat modeling, you know, 20 calls for. 21 Q. Okay. So the documents in that table, 22 do you know whether they relate to security design 23 implications versus data privacy concerns? 24 A. I feel like I just answered that 25 question. You know, I answered that I didn't look</p> <p style="text-align: center;">242</p>	<p>1 where I look at the presence of headings in 2 documents. 3 I've -- you know, as we've talked 4 about, looked at over 50 FSRs, right? There was a 5 simple point being made here that the FSRs, you 6 know, do lead a security team through a process 7 that includes, you know, things that, you know, 8 you would expect if you were -- you know, to see 9 if threat modeling. 10 So, you know, this -- again, was a 11 sort of a specific assessment of implementation of 12 threat modeling for an application. 13 This was the articulation of the fact 14 that the FSRs clearly called at the process level 15 for doing this. So this is just one of many 16 elements of, you know, my overall assessment that 17 threat modeling was occurring. 18 Again, something that was not present 19 in the securities statement, but that I do 20 believe, you know, the evidence in total, not this 21 sentence only, you know, clearly indicates that 22 they were doing. 23 BY MR. CARNEY: 24 Q. Okay. In that same paragraph 210, you 25 say, "Some of the FSRs also include design reviews</p> <p style="text-align: center;">244</p>

Gregory Rattray
2/12/2025

<p>1 by the architecture team further reflecting 2 consideration of security at the design stage." 3 Do you see that? 4 A. Yes. 5 Q. You didn't add a citation to that 6 sentence, did you? 7 A. I did not. 8 Q. Okay. Do you recall which FSRs you 9 had in mind here? 10 A. I don't recall the specific FSRs. 11 Q. And have you been able to look at any 12 design reviews by the architecture team? 13 A. It would be similar to the -- the 14 answer to the previous question. That was, you 15 know, not the point of this paragraph as a whole. 16 It's to the point that the FSR process 17 includes steps, and at times, you know, included, 18 you know, this step, design reviews by an 19 architecture team. 20 You know, my -- my approach is similar 21 to what's used in the industry. You're not trying 22 to check, you know, every -- you know, every 23 implementation down to the specific, you know -- 24 the specific -- you know, the follow-through on 25 every single specific FSR.</p> <p style="text-align: center;">245</p>	<p>1 Q. Well, let me just see if I can break 2 that down a little bit. 3 Would you agree with me that "threat 4 modeling" is a term of art in cybersecurity? 5 MR. TURNER: Object to form. 6 THE WITNESS: Yeah, term of art is -- 7 I'm not -- I'm not quite sure what you mean by 8 "term of art." 9 BY MR. CARNEY: 10 Q. It has a, sort of, generally accepted 11 meaning in cybersecurity, the term "threat 12 modeling"? 13 A. You know, "threat modeling" is one of 14 the terms in cybersecurity where there are a lot 15 of, you know, sort of interpretations of what 16 those words mean. 17 Yeah, you know, so I think a lot of 18 people have a -- you know, different 19 conceptualizations of what is meant when you use 20 the words "threat modeling" in cybersecurity. 21 Q. In your view, is threat modeling the 22 same as risk identification? 23 A. You know, threat is an element of 24 risk. They're not synonymous, but they're -- you 25 know, I guess I would consider them overlapping.</p> <p style="text-align: center;">247</p>
<p>1 The FSR process at the level of the 2 security statement, you know, demonstrates what 3 people reading that security statement would 4 expect from SolarWinds. 5 Q. Okay. So in reviewing the FSRs, you 6 assessed whether SolarWinds had the opportunity to 7 do threat modeling, but not whether they actually 8 did threat modeling, right? 9 A. No. You know, I looked at a lot of 10 FSRs. The FSRs, you know -- you know, show 11 activity that falls in, you know, the conduct of 12 threat modeling. 13 Again, you know, threat modeling is 14 not part of the securities statement, but there's 15 no reason to believe that the steps that are 16 outlined in the FSRs in the documentation that is, 17 you know -- you know, present -- you know, the 18 lengths of the documentation present in the FSRs, 19 you know, would not have occurred, right? 20 There's just every reason to believe 21 these FSRs are -- you know, the FSR process 22 itself, you know, threat modeling is -- it's a 23 strong process that there's no reason to believe 24 that the things that are called for, you know, 25 when they're present and the FSR didn't happen.</p> <p style="text-align: center;">246</p>	<p>1 Q. So what's the difference between 2 threat modeling and risk identification? 3 A. Well, risk identification, you know, 4 also includes the understanding of vulnerability. 5 You know, that's sort of classic terminology in 6 cybersecurity regarding risk is its threat and 7 vulnerability. 8 Q. Okay. Is there a difference between 9 threat modeling and risk mitigation? 10 A. In general in the field or -- 11 Q. In the cybersecurity field. 12 A. Yes, there's -- the two things, they 13 are different. "Threat modeling" could be an 14 element -- to me is a broader term of risk 15 mitigation. 16 Q. Are you aware of any steps that are 17 part of threat modeling as a cybersecurity best 18 practice? 19 MR. TURNER: Objection to form. 20 THE WITNESS: You know -- you know, I 21 think we've discussed this. That, you know, 22 threat modeling is -- you know, broadly, you know, 23 the identification of, you know, what act -- you 24 know, actors could do in terms of threatening a 25 specific, you know, organization.</p> <p style="text-align: center;">248</p>

Gregory Rattray
2/12/2025

<p>1 You know, identifying those as 2 security concerns working towards, you know -- in 3 the case of software development, you know, that 4 informing the software development. 5 BY MR. CARNEY: 6 Q. Okay. And I guess what I'm trying to 7 understand as -- you know, as a layperson is -- is 8 there, like, a typical, like, written output that 9 you would expect to see from a threat modeling 10 being conducted? 11 A. No. Not necessarily. You know, in 12 the broad conception of threat modeling, it's -- 13 you know, the -- in these processes, some of which 14 are in this paragraph, you know, being present is 15 indicative of, you know, getting the team to think 16 about how threat affects, you know, the 17 development in this case. 18 So specific artifacts, you know, are 19 not necessarily an outcome of threat modeling. 20 Q. When you've been involved in threat 21 modeling in the past, have you or a team working 22 for you typically produced a written output? 23 A. You know, I've seen outputs of a 24 formalistic threat modeling process, but that -- 25 I've also seen teams discuss, you know, threat</p> <p style="text-align: center;">249</p>	<p>1 in the deposition, but I see -- I see that 2 sentence here. 3 Q. Okay. I don't -- right now I don't 4 want to focus on the substance so much as I want 5 to understand your process for forming your 6 opinions about Mr. Colquitt's email in this 7 report. 8 And I'm wondering, when you are 9 discussing Mr. Colquitt's testimony about what the 10 email he wrote meant, were you sort of accepting 11 it at face value, his explanation? 12 MR. TURNER: You mean was he assuming 13 it was true? 14 MR. CARNEY: Right. 15 THE WITNESS: Again, I think -- I 16 think in this case it's important, because this, 17 you know, sentence talks both about an email and 18 then it talks about what he said in his deposition 19 when he wrote the email. 20 So, you know, in most of the sentence, 21 you know, where -- you know, I'm looking at two 22 sentences, but most of that is quotation. 23 MR. TURNER: I think the question is 24 simply whether you were assuming Mr. Colquitt was 25 truthful in his testimony.</p> <p style="text-align: center;">251</p>
<p>1 and, you know, not produce a formal -- a specific 2 output from that exercise. 3 Q. All right. And the times where you've 4 seen outputs of a formalistic threat modeling 5 process, what did that output look like? 6 A. You know, it could be lists of 7 specific actors. It could be lists of, you know, 8 threat actor, you know -- you know, approaches. 9 But, you know, more broadly, again, the concept of 10 threat modeling doesn't necessarily call for these 11 outputs. 12 And, you know, in the case that we 13 have in front of us, there isn't even a specific 14 identification that threat modeling is part of 15 what's promised in the secure -- you know, 16 asserted to be one of the -- SolarWinds's, you 17 know, activities in the securities statement. 18 Q. All right. Sir, if I could ask you to 19 look at paragraph 211 of your report -- 20 A. Uh-huh. 21 Q. -- page 115. And you have a 22 discussion there of Mr. Colquitt's email. 23 Do you see that? 24 A. Yes, I do. I should probably, you 25 know, look at both the email and his explanation</p> <p style="text-align: center;">250</p>	<p>1 THE WITNESS: I believe he was 2 truthful in his testimony, yes. I mean, that is 3 an assumption in the way I wrote my -- you know, 4 my report. 5 BY MR. CARNEY: 6 Q. And so specifically I want to focus 7 you on the sentence in the middle of paragraph 211 8 were you write, "In saying that, 'We are just 9 barely beginning to understand how teams are going 10 to be doing this activity,' he was not, 'talking 11 about doing a threat modeling itself,' but was 12 rather talking about how teams were going to be 13 documenting that activity." 14 For purposes of that sentence that you 15 wrote there, is it fair to say that you just 16 relied on Mr. Colquitt's explanation of what his 17 email actually meant? 18 A. You know, in terms of SolarWinds's 19 conducting threat modeling, I wasn't, you know, 20 solely reliant on this statement. We've talked a 21 lot about, you know, the evidence I relied upon to 22 find that, you know, threat modeling was occurring 23 in SolarWinds. 24 As we just stated, I believe, you 25 know, in terms of what I quoted, I believe he was</p> <p style="text-align: center;">252</p>

Gregory Rattray
2/12/2025

<p>1 telling the truth in his deposition.</p> <p>2 Q. And my question is: Have you seen any</p> <p>3 independent evidence to support Mr. Colquitt's</p> <p>4 statement that he was not talking about doing</p> <p>5 threat modeling itself but simply was talking</p> <p>6 about how teams were going to be documenting</p> <p>7 threat modeling?</p> <p>8 A. Again, you know, I just want to make</p> <p>9 sure that I'm, you know, correct about this. But</p> <p>10 if we had, you know, the timing of the email, you</p> <p>11 know, that would help.</p> <p>12 Because, you know, as I've said over</p> <p>13 and over again, the -- one of the primary sources</p> <p>14 of, you know, my finding that threat modeling was</p> <p>15 occurring is the presence of the -- the FSRs.</p> <p>16 You know, again, those were put in</p> <p>17 place just prior to the relevant period. But I --</p> <p>18 you know, I don't remember the exact timing of</p> <p>19 this statement.</p> <p>20 But, you know, those would certainly</p> <p>21 be independent of his assertion that they were not</p> <p>22 just talking about, you know -- you know, that</p> <p>23 they were doing threat modeling, and that what he</p> <p>24 was talking about was documenting the activity.</p> <p>25 Q. All right. So if the first sentence</p> <p style="text-align: center;">253</p>	<p>1 statement?</p> <p>2 MR. TURNER: Object to form. And</p> <p>3 foundation.</p> <p>4 THE WITNESS: As my report, you know,</p> <p>5 states, basically no security practice can, you</p> <p>6 know, conduct a perfect implementation of the set</p> <p>7 of things that are listed in the securities</p> <p>8 statement.</p> <p>9 Perfection is -- you know, is not the</p> <p>10 goal here. It's not the expectation of readers of</p> <p>11 the security statement.</p> <p>12 BY MR. CARNEY:</p> <p>13 Q. Fair enough. And I'm just trying</p> <p>14 to -- really right now I'm just trying to</p> <p>15 understand your opinion.</p> <p>16 A. Uh-huh.</p> <p>17 Q. Is it fair to say that it's your</p> <p>18 opinion that whatever lapses there were, were not</p> <p>19 pervasive or frequent at SolarWinds?</p> <p>20 A. I think that's fair. There were --</p> <p>21 you know, these were not pervasive, you know,</p> <p>22 systemic lapses, you know, to the extent that any</p> <p>23 of them existed.</p> <p>24 Q. And is it fair to say that it's your</p> <p>25 opinion that a small number of lapses over a</p> <p style="text-align: center;">255</p>
<p>1 of 211, you say, "With respect to Mr. Colquitt's</p> <p>2 email, it appears to me Mr. Graff takes this email</p> <p>3 out of context." So let's stop there.</p> <p>4 What do you mean that he took the</p> <p>5 email out of context? What's the context?</p> <p>6 A. Well, I mean, the context is explained</p> <p>7 by Mr. Colquitt in his deposition.</p> <p>8 Q. Okay. Is there any other context?</p> <p>9 MR. TURNER: Object to form.</p> <p>10 BY MR. CARNEY:</p> <p>11 Q. That you feel Mr. Graff failed --</p> <p>12 A. I -- I -- you know, I'd like to look</p> <p>13 at the email.</p> <p>14 Q. So I don't have a copy of the email,</p> <p>15 because you quoted most of it in your report.</p> <p>16 But --</p> <p>17 A. Yeah, I don't -- I don't have specific</p> <p>18 memory of the entire email.</p> <p>19 Q. Okay. Did you ever interview</p> <p>20 Mr. Colquitt?</p> <p>21 A. I did not.</p> <p>22 Q. Dr. Rattray, is it fair to say that it</p> <p>23 is your opinion that SolarWinds did not</p> <p>24 100 percent of the time conform to the</p> <p>25 cybersecurity practices described in the security</p> <p style="text-align: center;">254</p>	<p>1 multiyear period do not render this assertions in</p> <p>2 the security statement untrue?</p> <p>3 A. Can you just repeat one time for me?</p> <p>4 Q. Sure.</p> <p>5 Is it fair to say that it's your</p> <p>6 opinion that a small number of lapses over a</p> <p>7 multiyear period do not render the assertions in</p> <p>8 the security statement untrue?</p> <p>9 A. Excuse me. It's fair to say that, you</p> <p>10 know, the security statement calls for, you know,</p> <p>11 the presence of, you know, activity and practices.</p> <p>12 And that, you know, given the nature</p> <p>13 of cybersecurity, you.</p> <p>14 (Stenographer asks for clarification.)</p> <p>15 THE WITNESS: You will not achieve</p> <p>16 perfection, you know, in the implementation of</p> <p>17 those practices. You know, and so -- you know,</p> <p>18 that's -- that's sort of, you know, my opinion.</p> <p>19 And, you know, that's what -- you know, we're</p> <p>20 looking for here.</p> <p>21 I don't think any reader of the</p> <p>22 securities statement is looking to that statement</p> <p>23 to sort of hold -- you know, hold SolarWinds to</p> <p>24 its -- to its -- you know, to perfection in the</p> <p>25 execution.</p> <p style="text-align: center;">256</p>

Gregory Rattray
2/12/2025

<p>1 BY MR. CARNEY:</p> <p>2 Q. So is there a number of lapses that,</p> <p>3 in your opinion, would render the assertions in</p> <p>4 the security statement untrue?</p> <p>5 A. You know, that is not the way we look</p> <p>6 at, you know, sort of evaluating things like, you</p> <p>7 know, the presence of controls or activities,</p> <p>8 like, laid out in the security, you know -- in the</p> <p>9 security statement.</p> <p>10 So you have -- the determination is</p> <p>11 not numerical. I mean, I haven't done very -- you</p> <p>12 know, done large numbers of assessments and read</p> <p>13 large numbers of assessments on things like access</p> <p>14 controls.</p> <p>15 There's not a quantification, you</p> <p>16 know -- you know, involved in security assessment</p> <p>17 and, you know, evaluating the presence of</p> <p>18 practices.</p> <p>19 Q. So is it fair to say that there's a</p> <p>20 qualitative aspect of such an assessment?</p> <p>21 A. Yes, it is fair to say.</p> <p>22 Q. And so, for instance, if a company</p> <p>23 enforced their cybersecurity controls 99 percent</p> <p>24 of the time, but the 1 percent of the time they</p> <p>25 didn't was for the most critical systems, that</p> <p style="text-align: center;">257</p>	<p>1 THE WITNESS: Please repeat the</p> <p>2 question.</p> <p>3 BY MR. CARNEY:</p> <p>4 Q. Sure.</p> <p>5 Can you think of a type of</p> <p>6 cybersecurity mistake that is so serious that even</p> <p>7 one instance of it would indicate a major flaw</p> <p>8 with an organization's cybersecurity controls?</p> <p>9 MR. TURNER: Object to form.</p> <p>10 THE WITNESS: You know, I'm just</p> <p>11 trying to think of -- the answer is generally, no,</p> <p>12 right? Because, you know -- you know -- or maybe</p> <p>13 we have to talk about what "flaw" means.</p> <p>14 But, you know, cybersecurity is</p> <p>15 difficult, and perfection is basically impossible</p> <p>16 to achieve. So the fact that there's a flaw, that</p> <p>17 does not mean that -- you know, the</p> <p>18 organization -- you know, again, we're in a</p> <p>19 hypothetical here -- isn't actually good at that</p> <p>20 control, right?</p> <p>21 You know, I cite the example, you</p> <p>22 know, in my report of an error that occurred in</p> <p>23 the World Series by a fielder that hadn't had any</p> <p>24 errors, right? So that was a pretty serious flaw</p> <p>25 but, you know, like, flaws happen, right?</p> <p style="text-align: center;">259</p>
<p>1 would matter in a cybersecurity assessment, right?</p> <p>2 A. You know, in terms of the assessment</p> <p>3 of the security statement, which is not about sort</p> <p>4 of -- it's about the presence of processes, right?</p> <p>5 It says SolarWinds's -- you know --</p> <p>6 you know, I don't want to -- to the -- you know,</p> <p>7 it says -- I just want to be precise -- you know,</p> <p>8 that SolarWinds is conducting activities.</p> <p>9 You know, the magnitude -- it does not</p> <p>10 discuss, you know -- again, I have to take a quick</p> <p>11 look, but I do not think it discusses, you know,</p> <p>12 the -- the magnitude of anything.</p> <p>13 It discusses, you know, activities</p> <p>14 that SolarWinds conducts. So in terms of</p> <p>15 assessing this statement and what it asserts, the</p> <p>16 magnitude of any specific, you know, problem that</p> <p>17 might be identified actually is not relevant to</p> <p>18 the securities statement.</p> <p>19 Q. This is a hypothetical --</p> <p>20 A. Uh-huh.</p> <p>21 Q. -- but can you think of a type of</p> <p>22 cybersecurity mistake that is so serious that even</p> <p>23 one instance of it would indicate a major flaw</p> <p>24 with an organization cybersecurity controls?</p> <p>25 MR. TURNER: Object to form.</p> <p style="text-align: center;">258</p>	<p>1 So I don't think it's -- you know,</p> <p>2 certainly a singular incident isn't sort of a</p> <p>3 reflection of, you know, on -- isn't a reflection</p> <p>4 on a judgment related to the -- you know --</p> <p>5 whether a control structure is there or, you</p> <p>6 know -- yeah, is there.</p> <p>7 BY MR. CARNEY:</p> <p>8 Q. And just for the record, that</p> <p>9 reference to that error was a personal affront to</p> <p>10 me, and it was painful so soon after the World</p> <p>11 Series, but that's --</p> <p>12 A. I understand.</p> <p>13 Q. -- neither here nor there.</p> <p>14 So let me give you a hypothetical.</p> <p>15 Let's say -- this is a hypothetical. U.S.</p> <p>16 government accidentally leaks the passwords that</p> <p>17 are needed to use the nuclear weapons, like the --</p> <p>18 what is it? -- the biscuit?</p> <p>19 A. It's not a biscuit. But the</p> <p>20 briefcase.</p> <p>21 Q. The briefcase?</p> <p>22 A. Briefcase moves around with the</p> <p>23 President.</p> <p>24 Q. Got it.</p> <p>25 A. Yes.</p> <p style="text-align: center;">260</p>

Gregory Rattray
2/12/2025

<p>1 Q. And it happens only once. 2 Would you agree that despite this 3 mistake not being frequent, it could still 4 indicate a significant issue with the government 5 cybersecurity controls? 6 MR. TURNER: I'm going to object to 7 form. 8 A "significant issue," do you mean a 9 consequential one or do you mean a pervasive one? 10 BY MR. CARNEY: 11 Q. Well, you can answer. 12 Significant in that it's important. 13 A. Yeah, I mean, you know, the 14 distinction being made, you know, "significant" 15 can be -- you know, an issue of magnitude, which 16 is -- we were just discussing, you know, a 17 singular mistake doesn't, you know, mean a 18 control -- control process is not strong. 19 You know, mistakes get made. You 20 know, its magnitude could be grave in a single 21 instance, but it's not -- you know, not an 22 indication of a pervasive failure of, you know, 23 any given process or control. 24 Q. If the military attache that was 25 supposed to be guarding that briefcase routinely</p> <p style="text-align: center;">261</p>	<p>1 the -- the bad event was the result of clearly 2 numerous indications of, you know, misapplication 3 of the -- the control, you know, you would want to 4 be reviewing that, you know, when you had the 5 incident. 6 You know, that's my sort of 7 perspective on that hypothetical. 8 Q. But in the original hypothetical, if 9 it was -- only happened one time, that wouldn't 10 warrant the review of the controls? 11 A. I didn't say it wouldn't warrant a 12 review. 13 Q. And it could possibly be evidence of a 14 serious problem with the controls, right? 15 A. Yeah. Again, you would look at the 16 context. You know, in most cases -- and, again, 17 we're talking very hypothetically, so whether this 18 applies to SolarWinds or not, it largely doesn't 19 apply to the security statement for the reasons 20 I've said, which is the security statement is 21 about the presence of activities and programs. 22 You know, if a serious error was to 23 occur, there would be a review. You know, yeah. 24 So, you know, that's generally what happens in, 25 you know, these types of processes like your</p> <p style="text-align: center;">263</p>
<p>1 left it in the restroom but only one time did 2 someone take it, would that be -- could that be 3 indicative of a systemic problem, even though it 4 was only leaked that once? 5 MR. TURNER: Again, I'm sorry. But he 6 routinely left it unattended in the restroom? 7 That was your... 8 MR. CARNEY: Right. 9 BY MR. CARNEY: 10 Q. But it was only stolen once. 11 MR. TURNER: But it was done 12 routinely? 13 MR. CARNEY: Right. 14 MR. TURNER: Okay. 15 THE WITNESS: Again, we're talking 16 about -- obviously we're talking about -- 17 BY MR. CARNEY: 18 Q. A different hypothetical? 19 A. -- a hypothetical, right, and actually 20 knowing people that have been responsible for 21 carrying that briefcase personally. You know, 22 there's a lot of process that goes into avoiding, 23 you know, routine misbehavior like that. 24 You know, because it's a -- an error 25 would be grave. So, you know, if -- you know, if</p> <p style="text-align: center;">262</p>	<p>1 hypothetical. 2 Certainly I am sure that if the 3 briefcase was, you know -- you know, lost, it 4 would be a very significant review of why that 5 occurred. 6 Q. And the briefcase is the football, 7 right, and the biscuit is the thing the President 8 carries, right? 9 A. The briefcase is sometimes referred to 10 as a football, right, you know. 11 Q. So, sir, if I could ask you to look at 12 paragraph 104. This is the bottom of page 57, and 13 Exhibit 1 and carries over to page 58. 14 A. I did it again [speaking sotto voce]. 15 MR. TURNER: Do you just want to give 16 him a chance to read it? 17 MR. CARNEY: Yeah. 18 THE WITNESS: So we're gonna -- we're 19 gonna discuss material in paragraph 104? 20 BY MR. CARNEY: 21 Q. Yes. 22 A. Okay. 23 (Pause for reading/reviewing.) 24 A. Okay. I would have looked through 25 paragraph 104.</p> <p style="text-align: center;">264</p>

Gregory Rattray
2/12/2025

<p>1 Q. Okay. At the end of paragraph 104, 2 the last sentence you say, "Nor does Mr. Graff 3 identify any benchmark for an expected or 4 acceptable error rate against which to judge 5 implementation of SolarWinds's controls even 6 though he acknowledges repeatedly that errors and 7 lapses occur in any cybersecurity program." 8 A. Right. 9 Q. I want to ask you: Is it your opinion 10 that Mr. Graff should have identified an 11 acceptable error rate against which to judge the 12 implementation of SolarWinds's controls? 13 A. Yes, it is. Because Mr. Graff is 14 making assertions around pervasiveness and 15 systemic issues, which inherently involve, you 16 know, a -- you know, some sort of expectation of 17 what constitutes pervasive versus systemic. 18 Q. Okay. And you yourself did not 19 calculate acceptable error rate, did you? 20 A. Yeah, because we were doing very 21 different things. 22 Q. And in your concept of the acceptable 23 error rate, what is the numerator in the rate? 24 A. I didn't make any assertions around 25 pervasiveness or systemic. And I -- and I -- so</p> <p style="text-align: center;">265</p>	<p>1 MR. CARNEY: What is the numerator, 2 what is the denominator for the -- 3 THE WITNESS: Yeah, I don't know for a 4 given control. 5 (Simultaneous unreportable crosstalk 6 occurs among parties.) 7 THE WITNESS: If the denominator is 8 tens of thousands of, you know, instances of 9 occurrence, how many errors, you know -- I don't 10 -- again, I can't in this question say if that 11 number is 10, 100. You know, those sorts of 12 things. 13 And what that number is, is very 14 dependent on what control and situation. Even the 15 factors that go into determining -- determining if 16 it's 10 or 100. 17 MR. TURNER: Can I try? 18 Go ahead if you want. I think I know 19 what you're getting at. 20 BY MR. CARNEY: 21 Q. Yeah. And I'm not looking for you to 22 quantify it or give me a number between 1 and a 23 million. 24 A. Right. 25 Q. I just want to know what types of</p> <p style="text-align: center;">267</p>
<p>1 for the places where Mr. Graff is asserting that 2 something is pervasive or systemic, I'd have to 3 look at that specific situation. 4 But, you know, it certainly wasn't 5 within, you know, the -- the task I had at hand to 6 determine those rates. 7 Q. Right. And I'm just trying to 8 understand the error rate that Mr. Graff -- that 9 you feel he should have calculated. 10 What would be the numerator in that 11 rate that he should have calculated? 12 By that I don't mean the actual 13 number. I mean what category of items would go 14 into the numerator? 15 A. Again, this is completely contextually 16 dependent. 17 MR. TURNER: I think you might be 18 talking past each other. 19 Are you saying, like, what is the 20 numerator? 21 MR. CARNEY: Right. 22 BY MR. CARNEY: 23 Q. What is in the formula? 24 MR. TURNER: If errors are systemic, 25 what is the -- what is the numerator?</p> <p style="text-align: center;">266</p>	<p>1 activities go into the numerator versus into the 2 denominator in calculating that error rate? Is it 3 incidents go into the numerator? 4 A. Controls have such -- you know, there 5 are a lot of controls, and even the data that is 6 used for those controls varies widely. I don't 7 know what goes into the numerator for any -- 8 unless we talk about a specific control. 9 Q. All right. So is it fair to say that 10 the error rate that you say that Mr. Graff should 11 have calculated, you yourself don't know how that 12 would have been calculated? 13 A. No. That's not what I said. I said 14 you need to give -- you need to talk to me about a 15 control, and I'll talk to you about how -- how I 16 might go about it theoretically given that that 17 was not the task that I had at hand. 18 Q. Okay. Let's use passwords then. 19 So how would you calculate an error 20 rate for the password policy? 21 A. You know, again, you know, you would 22 look at, you know, how many instances of -- again, 23 the -- you know, the password policy, you know, 24 has different stages. 25 But let's just say the number of times</p> <p style="text-align: center;">268</p>

Gregory Rattray
2/12/2025

<p>1 you issued a new employee password and you would 2 have -- you know, you would seek to devine a 3 denominator -- you know, you would -- data that 4 gave you sort of a denominator that -- to that. 5 And then, you know, if you were going 6 to say it was systemic, you would work at, you 7 know, probably through a structure, you know, 8 of -- you know, interaction of, like, what 9 percentage -- I mean, we have risk metrics all the 10 time. 11 So you sort of set thresholds for, 12 okay, you know, 5 percent error rate, you know, 13 starts to get on a -- you know -- on a risk 14 reporting, you know, ledger, right? 15 So, you know, it is certainly possible 16 and happens quite frequently in terms of measuring 17 control implementation that metrics are put in 18 place that include determinations and numerators 19 that are relevant to the denominators. 20 MR. TURNER: Just to -- I just want to 21 be -- just to be clear. 22 THE WITNESS: Hopefully -- I'm trying 23 to answer the question. 24 MR. TURNER: Just to be sure, by 25 "numerator," he's talking the errors, like the</p> <p style="text-align: center;">269</p>	<p>1 (Whereupon, a recess was taken at 2 5:27 p.m.) 3 THE VIDEOGRAPHER: The time right now 4 is 5:48 p.m. 5 We are back on the record. 6 BY MR. CARNEY: 7 Q. All right. Dr. Rattray, I'm going to 8 ask you a little bit about password protection. 9 Do you agree that, sort of, after the 10 fact, incident response cannot fully compensate 11 for inadequate password protection? 12 A. I think it's very contextual. 13 Q. Okay. Well, all right. Do you agree 14 that poor password security can lead to breaches 15 that happen too quickly or too stealthily for 16 incident response to mitigate them effectively? 17 MR. TURNER: Objection to form. 18 THE WITNESS: You know, again, we 19 should look at the specific context. You know, 20 again, these are a very, sort of, abstract 21 question. 22 BY MR. CARNEY: 23 Q. Right. And in fairness, you're an 24 expert witness, so I'm -- 25 A. Uh-huh.</p> <p style="text-align: center;">271</p>
<p>1 noncompliant passwords -- 2 A. Right- 3 Q. -- and the total number -- 4 (Simultaneous unreportable crosstalk 5 occurs among parties.) 6 (Stenographer requests one speaker at a 7 time.) 8 THE STENOGRAPHER: It's not clear for 9 the record. 10 MR. TURNER: Do you want me to repeat? 11 THE STENOGRAPHER: Please. 12 MR. TURNER: Just I want to make 13 clear, I think by "numerator," we're talking about 14 the number of noncompliant passwords, the 15 denominator would be the total number of passwords 16 in that particular example. 17 THE WITNESS: Yeah, I'm good -- I 18 agree with that. 19 MR. CARNEY: Okay. All right. It's 20 been an hour, I think. 21 We can take a break. Thanks. 22 THE WITNESS: Okay. 23 THE VIDEOGRAPHER: The time right now 24 is 5:27 p.m. 25 We are off the record.</p> <p style="text-align: center;">270</p>	<p>1 Q. -- permitted to ask these kind of 2 abstract questions. 3 A. Okay. 4 Q. So I'm talking just at a general 5 level, can there be situations where poor password 6 security leads to a breach that just happens too 7 quickly for the incident response to mitigate it 8 effectively? 9 Are you aware of such situations? 10 MR. TURNER: Object to form. 11 THE WITNESS: Yeah, I mean, I think 12 that the general proposition that a control lapse 13 could lead to a breach that -- you know, evolved 14 quickly, you know, it's not just password 15 protection. 16 You know, other security controls, you 17 know, could lead to, you know -- again, very 18 theoretically, could lead to rapidly, you know, 19 evolving situations. 20 BY MR. CARNEY: 21 Q. And what other security controls are 22 you thinking of? 23 A. I'm just trying to -- I mean, almost 24 all security controls, if they fail dramatically, 25 can be highly problematic.</p> <p style="text-align: center;">272</p>

Gregory Rattray
2/12/2025

<p>1 So, yeah, you know, misconfiguration 2 on a -- you know, on a device or an unpatched 3 system, you know, would be other types of security 4 controls that could lead to a similar situation. 5 Q. Okay. And do you agree that once 6 attackers gain valid login credentials, they can 7 often escalate privileges and move laterally 8 across a network in minutes? 9 MR. TURNER: Objection to form. 10 THE WITNESS: Yeah, that's not 11 generally how it occurs. So, yeah, generally I 12 don't agree with that. 13 BY MR. CARNEY: 14 Q. I don't think I used the word 15 "generally" -- 16 A. Okay. Okay. All right. 17 MR. TURNER: What are you asking, 18 Chris? That sometimes an attacker can get in and 19 escalate privileges and move laterally across a 20 network? 21 MR. CARNEY: In minutes, right, yes. 22 THE WITNESS: Yeah, that's why I said, 23 you know -- 24 MR. TURNER: Is that possible? Is 25 that the question?</p> <p style="text-align: center;">273</p>	<p>1 know, you layer security controls, and, you know, 2 you can have compensating controls. 3 And, you know, you look at those, and 4 if you're looking at a specific situation and, you 5 know, hopefully -- you know, you're looking to 6 have a layered set of controls that, you know, if 7 one doesn't work well, others compensate for that. 8 Q. Right. And do you agree that even if 9 an incident response team detects a breach 10 quickly, damage may already be done? 11 A. Not necessarily, right? You know, 12 again, compensating controls that limit damage for 13 a breach are not just incident response. 14 Q. Do you agree that a password leak may 15 be used months later bypassing any immediate 16 response efforts? 17 MR. TURNER: I don't even understand 18 the grammar of the question. 19 But object to the form. 20 THE WITNESS: Could you just restate, 21 please. 22 BY MR. CARNEY: 23 Q. Yeah, a leaked password, someone could 24 sit on it for months and not use it until months 25 after it was leaked, right?</p> <p style="text-align: center;">275</p>
<p>1 BY MR. CARNEY: 2 Q. It happens, right? 3 A. Yeah. Rarely. 4 Q. I mean, if -- you know, if you want me 5 to tell you -- you know, the purpose of the -- I'm 6 not required to -- 7 A. Uh-huh. 8 Q. -- but the -- isn't it true that after 9 the fact, incident remediation is not a substitute 10 for strong password protection, right? Would you 11 agree with that statement? 12 MR. TURNER: Objection. 13 THE WITNESS: Um -- 14 MR. TURNER: Objection to the form of 15 the question. 16 THE WITNESS: I wouldn't, because 17 security controls are not considered substitutes 18 for each other. 19 BY MR. CARNEY: 20 Q. Right. So you couldn't just say, we 21 have quick remediation procedures, therefore, we 22 don't need password protection, right? 23 A. In my estimation, you know, I never 24 heard a conversation where that sort of 25 consideration has ever come up. So I just -- you</p> <p style="text-align: center;">274</p>	<p>1 A. Yeah, theoretically that could happen. 2 Q. And is it fair to say that you accept 3 that at least in one incident in 2019, a security 4 researcher reported finding a SolarWinds password 5 contained in the code repository that had 6 accidentally been made publicly available on 7 GitHub? 8 A. Yes, I remember that specific 9 situation. 10 Q. And just so I understand your opinion 11 about that, is it your opinion that this incident 12 was quickly remediated after the external security 13 researcher reported it? 14 A. That's my understanding is it was 15 quickly remediated. 16 Q. And why does it matter that it was 17 quickly remediated after the discovery? 18 A. You know, I think -- you know, we 19 should probably look specifically at how I 20 phrased -- 21 Q. Sure. 22 A. -- phrased that, because I think 23 you're asking for -- you're asking me -- 24 Q. Sure. 25 A. -- for why I said that, right? So can</p> <p style="text-align: center;">276</p>

Gregory Rattray
2/12/2025

<p>1 we point -- can you point me to where this is 2 discussed?</p> <p>3 Q. Sure. I think it's in paragraph 132 4 of your report. Exhibit 1.</p> <p>5 A. Uh-huh. Yeah, we're in -- that's the 6 right area.</p> <p>7 Q. Page 72.</p> <p>8 A. Yes. So I'm reading, yeah, 9 paragraph 132.</p> <p>10 And, you know, is the question why I 11 mentioned the fact that the -- the incident was 12 remediated immediately after?</p> <p>13 Q. Well, we can start with that. 14 Why did you mention it?</p> <p>15 A. Because -- yeah, I mean -- in numerous 16 places in Mr. Graff's report, he talks to -- about 17 the severity of incidents, you know, and the fact 18 that, you know, this incident was, you know, 19 remediated immediately, you know, is relevant to, 20 you know, the judgment of whether it was, you 21 know -- you know, the magnitude of the risk was 22 high.</p> <p>23 It also, you know, shows more 24 generally that -- you know, SolarWinds as a 25 security practice, you know, again, more</p> <p style="text-align: center;">277</p>	<p>1 negative consequences here.</p> <p>2 So, you know, the fact that they -- I 3 actually think that the fact that they remediated 4 it quickly is just evidence that they -- they were 5 constantly looking for problems and acting quickly 6 when they can.</p> <p>7 I actually don't -- you know, again, 8 because it was another compensating control, the 9 two layers of control quickens a response and, you 10 know, digital signature, you know, meant that -- 11 this incident wasn't significant.</p> <p>12 Q. Okay. You mentioned digital 13 signature --</p> <p>14 A. Uh-huh.</p> <p>15 Q. -- was that one of the compensating 16 controls that, for lack of a better term, failed 17 in connection with the Sunburst incident, as you 18 understand it?</p> <p>19 MR. TURNER: Objection to form. 20 THE WITNESS: No.</p> <p>21 BY MR. CARNEY:</p> <p>22 Q. You don't recall any aspect of that 23 incident relating to the digital signature?</p> <p>24 MR. TURNER: Different question. 25 Go ahead.</p> <p style="text-align: center;">279</p>
<p>1 generally, you know, had layers of controls, had a 2 series of compensating controls to deal with, you 3 know, any singular isolated lapse like the one in 4 this incident.</p> <p>5 Q. Okay. And in your view as someone in 6 the cybersecurity field, why is it important that 7 a password leak be remediated quickly?</p> <p>8 A. You know, I think, you know, the 9 general practice in the field is to try to 10 remediate any, you know, security lapse as fast as 11 possible.</p> <p>12 Q. All right. So we're talking about 13 this particular --</p> <p>14 A. Uh-huh.</p> <p>15 Q. -- one here.</p> <p>16 What are the consequences of not 17 remediating it quickly?</p> <p>18 A. You know, are you asking what -- in 19 this specific context, what might have happened 20 badly if they didn't have quick remediation?</p> <p>21 Q. Right.</p> <p>22 A. As it states in the report, it was 23 another compensating control around digital 24 signature that also, you know, would have -- you 25 know, remediated the -- you know, the potential</p> <p style="text-align: center;">278</p>	<p>1 THE WITNESS: Yeah, you know -- you 2 know, my understanding of the Sunburst incident 3 is, you know, the highly sophisticated Russian, 4 you know, intelligence agency that intruded on 5 SolarWinds got inside their software development 6 process.</p> <p>7 And, you know -- you know, in the 8 distribution of that, you know -- you know, 9 distributed software that, you know, I don't have 10 the forensics, but probably was digitally signed. 11 So it's a very different sort of situation.</p> <p>12 BY MR. CARNEY:</p> <p>13 Q. Okay. If a cybersecurity incident 14 such as a password leak is not remediated quickly, 15 what can happen? What are the consequences?</p> <p>16 MR. TURNER: Objection to form.</p> <p>17 THE WITNESS: Yeah, that is very 18 dependent on the situation.</p> <p>19 BY MR. CARNEY:</p> <p>20 Q. I'm trying to understand why it 21 mattered to you that they remediated the password 22 leak quickly? How does that reflect on whether 23 they were following their password practices or 24 not?</p> <p>25 A. As I said, you know, and Mr. Graff in</p> <p style="text-align: center;">280</p>

Gregory Rattray
2/12/2025

<p>1 numerous cases, you know, discusses, you know --</p> <p>2 you know, these particular incidents and makes</p> <p>3 assertions around their magnitude and severity.</p> <p>4 And, you know, this particular, you</p> <p>5 know, callout on the compensating controls</p> <p>6 including the speed of investigation, you know,</p> <p>7 both sort of addresses the fact that this</p> <p>8 wasn't -- you know, a major or serious incident.</p> <p>9 And more generally, you know, shows</p> <p>10 that SolarWinds had strong security practice,</p> <p>11 which would then -- you know, I mean that -- you</p> <p>12 know, in areas like password security or across</p> <p>13 the full set of, you know, activities in the</p> <p>14 security statement that this was a practice that</p> <p>15 was strong and one would expect was doing the</p> <p>16 things in the security statement.</p> <p>17 Q. Did you review any risk acceptance</p> <p>18 forms in conjunction with your work in this case?</p> <p>19 A. Yes, I did.</p> <p>20 Q. And why did you review risk acceptance</p> <p>21 forms?</p> <p>22 A. You know, in some of the incidents, a</p> <p>23 determination was made that, you know -- you know,</p> <p>24 there was a risk acceptance that, you know -- that</p> <p>25 helped address what happened, you know, or was</p> <p style="text-align: center;">281</p>	<p>1 MR. TURNER: Okay.</p> <p>2 BY MR. CARNEY:</p> <p>3 Q. So -- and I just want to ask you about</p> <p>4 risk acceptance forms generally.</p> <p>5 A. Uh-huh.</p> <p>6 Q. Do you agree that risk acceptance</p> <p>7 forms can show that an organization identified</p> <p>8 certain risks stemming from violation of a policy?</p> <p>9 A. Just risk acceptance forms that -- you</p> <p>10 know, are a -- you know, the form itself is sort</p> <p>11 of the documentation of a process that, you know,</p> <p>12 if an activity is deemed risky, judgments are made</p> <p>13 about, you know, what is acceptable behavior, you</p> <p>14 know, or the acceptable path or not going forward</p> <p>15 in terms of the risk acceptance process.</p> <p>16 And, you know, again, the form is the</p> <p>17 documentation of that process occurring and</p> <p>18 decisions being made.</p> <p>19 Q. Got it.</p> <p>20 And all I'm trying to understand is</p> <p>21 that -- will that form contain an assessment of</p> <p>22 the risks that you face if you violate the given</p> <p>23 policy?</p> <p>24 A. Yeah. I mean, usually I think it</p> <p>25 does. Again, are we talking in this specific case</p> <p style="text-align: center;">283</p>
<p>1 part of addressing what happened in the incident.</p> <p>2 Q. Do you recall which incident?</p> <p>3 A. I believe, but I want to confirm, you</p> <p>4 know, that this is the incident that involves the</p> <p>5 access of developers -- in the billing system or</p> <p>6 the -- the -- yeah, the -- the billing -- you</p> <p>7 know, the billing system, you know, event or, you</p> <p>8 know, situation.</p> <p>9 Q. So doing development work in the</p> <p>10 production environment; is that fair to say?</p> <p>11 A. I just want to make sure that I'm</p> <p>12 correct and, you know, that is one of the places</p> <p>13 that I looked at risk assessment. Pretty sure.</p> <p>14 There's a lot of detail in this case.</p> <p>15 Q. So if you look at, I think,</p> <p>16 paragraph 123 of your report --</p> <p>17 A. Uh-huh.</p> <p>18 Q. -- on page 68.</p> <p>19 A. Yeah, okay. So that's correct.</p> <p>20 Q. So -- I --</p> <p>21 MR. TURNER: I just want to make sure</p> <p>22 I'm looking at the right part.</p> <p>23 What are you looking at, Chris?</p> <p>24 MR. CARNEY: So if you look at the</p> <p>25 bottom of page 68.</p> <p style="text-align: center;">282</p>	<p>1 about this specific incident or generally?</p> <p>2 Because risk acceptance forms are per- -- you</p> <p>3 know, risk acceptance is a common way of dealing</p> <p>4 with, you know, security situations and risks.</p> <p>5 And, again, it -- I've seen it in many</p> <p>6 different contexts.</p> <p>7 So are we talking about a general</p> <p>8 process or the specific case here?</p> <p>9 Q. So right now I'm asking generally.</p> <p>10 A. Okay.</p> <p>11 Q. And I'll ask you specifically --</p> <p>12 A. Right.</p> <p>13 Q. -- in a second.</p> <p>14 So just generally I'm trying to</p> <p>15 understand, do risk acceptance forms generally</p> <p>16 show the risks that a company will face if they</p> <p>17 were to accept the given risk and violate the</p> <p>18 policy?</p> <p>19 A. Yeah, they -- I mean, often they're</p> <p>20 not, sort of, you know, judgments on the policy as</p> <p>21 a whole. You know, they tend to be, again,</p> <p>22 context driven and situation specific.</p> <p>23 But, you know, yes, you know, in my,</p> <p>24 you know, experience, you know, this process and</p> <p>25 those forms do identify what risks are being, you</p> <p style="text-align: center;">284</p>

Gregory Rattray
2/12/2025

<p>1 know, considered in -- for acceptance or not 2 generally. 3 Q. All right. Maybe it's easier, I'll 4 just show you the specific example that we're 5 talking about -- 6 A. Uh-huh -- 7 Q. -- here. 8 A. -- right. 9 (Whereupon, Exhibit 17 is marked for 10 identification.) 11 BY MR. CARNEY: 12 Q. And just for the record, what you've 13 been handed as Exhibit 17 is the native version of 14 a document that had Bates stamp SW-SEC00168780. 15 And it was a July 2020, RAF or risk acceptance 16 form spreadsheet. And it was cited in Mr. Graff's 17 report. 18 And I want to ask you, sir -- and just 19 so you -- it's a sort of a big spreadsheet -- 20 A. Uh-huh. 21 Q. -- just the way it's set up is that 22 each row, if you will, spans two pages. So if you 23 could turn to the third page. 24 A. So page 3 of 8 in this -- 25 Q. Page 3 of 8 in this exhibit.</p> <p style="text-align: center;">285</p>	<p>1 spreadsheet shows that SolarWinds accepted the 2 risk that developers had write access to 3 production data? 4 MR. TURNER: Generally, or are you 5 talking about in this specific instance? 6 MR. CARNEY: In this specific 7 instance, yes. 8 Thank you. 9 THE WITNESS: Yes. 10 BY MR. CARNEY: 11 Q. And do you agree that that same cell 12 that we're looking at here, this would be 13 Column C -- 14 A. Uh-huh. 15 Q. -- states that, "APIs have write 16 permissions which are not used or needed"? 17 A. Yes. I mean, this sentence has -- you 18 know, they are using the APIs just to pull data, 19 but those three APIs have write permissions which 20 are not used. 21 Q. And do you agree that access that is 22 not used or needed is not the least necessary 23 amount of access? 24 MR. TURNER: Object to form. 25 THE WITNESS: Not necessarily. You</p> <p style="text-align: center;">287</p>
<p>1 A. Uh-huh. 2 Q. And you'll see Row 9, the BizApps 3 Billing DB. 4 Do you see that? 5 A. Yeah, I do. 6 Q. And then if you want to see the entire 7 row, you would turn to page 4 of 8. 8 A. Okay. Yeah. 9 Q. And if you look in Column M on page 4, 10 you see, "11/18/19. Risk reviewed and accepted by 11 Tim Brown." 12 Do you see that? 13 A. I mean, I think -- I just want to make 14 sure. 15 So I see Columns J and K. K has, you 16 know, Tim Brown's name on Approved By. Uh-huh, 17 yeah, if that's what the question was, the 18 answer's yes. 19 Q. Okay. And then if you look at 20 Column M, that has under "Compensating Control," 21 there's actually a date and a notation, "Risk 22 reviewed by and accepted by Tim Brown." 23 Do you see that? 24 A. I do. 25 Q. So would you agree that Row 9 of this</p> <p style="text-align: center;">286</p>	<p>1 know, my understanding of this situation is the 2 way that technology was set up, you know, at the 3 time, you know, you didn't have a choice to have, 4 you know -- you know, to use the technology 5 without write permissions. 6 So, you know, all sort of least 7 privilege and rule-based access is sort of in the 8 context of, you know, what you need to do to do 9 your job. And the developers, to do their job, 10 needed to use these APIs. 11 BY MR. CARNEY: 12 Q. Is it your understanding that 13 SolarWinds had a policy to separate development 14 from production? 15 MR. TURNER: Object to form. 16 Yeah, in the network security portion, 17 I believe of the security -- let's just check 18 that. 19 BY MR. CARNEY: 20 Q. Of Exhibit 5. 21 A. Yeah. Yeah, it's in the network 22 security portion of the security statement. 23 Q. And are you specifically referring to 24 the first sentence of the second paragraph -- 25 A. Yeah.</p> <p style="text-align: center;">288</p>

<p>1 Q. -- where it says, "SolarWinds 2 maintains separate development and production 3 environments"?</p> <p>4 A. Yes, I am.</p> <p>5 Q. Do you agree that the risk outlined 6 here where developers had access to production 7 data is inconsistent with separating development 8 from production?</p> <p>9 A. Are we talking about the write aspect 10 of it or some other element of this?</p> <p>11 Q. So we are talking about the developers 12 having read and write access to production data 13 where they were doing their development work.</p> <p>14 You recall this from our discussion 15 earlier, right?</p> <p>16 MR. TURNER: "You" here is asking -- 17 even with read access, would be reading production 18 data.</p> <p>19 So I think he's asking do your 20 questions relate to this or another aspect of --</p> <p>21 THE WITNESS: Yeah, I mean, we're on 22 this notion that, you know, the risk was poised 23 because they had write access, and then we, you 24 know, pivoted to development and production 25 environment.</p> <p style="text-align: center;">289</p>	<p>1 That's different than developers as 2 people conducting activity, you know -- you know, 3 developers inside the production environment. 4 It's -- to my mind, an apple and an orange.</p> <p>5 Q. So you don't believe that SolarWinds 6 had a -- relating to your second point, a policy 7 of preventing people conducting development inside 8 the production environment?</p> <p>9 MR. TURNER: Objection to form.</p> <p>10 You're asking was there a policy 11 beyond what's in the securities statement?</p> <p>12 MR. CARNEY: No.</p> <p>13 MR. TURNER: Okay.</p> <p>14 THE WITNESS: Yeah, are you saying 15 that the securities statement in some way 16 obligated, you know, SolarWinds to prohibit, you 17 know, developers from operating in the production 18 environment? Is that --</p> <p>19 BY MR. CARNEY:</p> <p>20 Q. Yes.</p> <p>21 A. -- is that the question?</p> <p>22 Q. Exactly.</p> <p>23 A. I don't see that language in the 24 security statement. But, again, maybe I need to 25 read more -- more thoroughly every sentence.</p> <p style="text-align: center;">291</p>
<p>1 You know, as something SolarWinds -- 2 I'm just trying to relate the two.</p> <p>3 BY MR. CARNEY:</p> <p>4 Q. Okay. So, well, let me break it apart 5 then.</p> <p>6 Do you agree that these developers 7 had -- were performing development work in a 8 production environment?</p> <p>9 A. Yes.</p> <p>10 Q. Okay. And do you agree that 11 SolarWinds had a policy against allowing 12 development in production environment?</p> <p>13 MR. TURNER: Chris, are we talking 14 about the security policy -- 15 (Simultaneous unreportable crosstalk 16 occurs among parties.)</p> <p>17 THE WITNESS: Yeah --</p> <p>18 BY MR. CARNEY:</p> <p>19 Q. Yes.</p> <p>20 A. And, again, SolarWinds had a network 21 security, you know -- set in the network security 22 portion of its securities statement that it 23 maintains network, you know, by implication, 24 separation of development and production network 25 environments.</p> <p style="text-align: center;">290</p>	<p>1 Because the network security element of it 2 doesn't -- doesn't address the people aspect of 3 this.</p> <p>4 It talks about -- it's about network 5 separation.</p> <p>6 Q. All right. Well, so let -- let me ask 7 you then: Do you agree as a cybersecurity 8 professional that it is -- I'm talking about best 9 practices here --</p> <p>10 A. Uh-huh.</p> <p>11 Q. -- that it's not part of a secure 12 software development lifecycle to develop inside 13 the production environment?</p> <p>14 MR. TURNER: Object to form.</p> <p>15 THE WITNESS: Again, are we talking 16 separate from the security statement and just sort 17 of abstractly about best practice?</p> <p>18 BY MR. CARNEY:</p> <p>19 Q. I'm not gonna -- I'm not gonna argue 20 with you about what the security statement covers, 21 so right now I just want to ask you about best 22 practices.</p> <p>23 You can put aside the security 24 statement for a second.</p> <p>25 Do you agree that it is not part of a</p> <p style="text-align: center;">292</p>

1 secure software development lifecycle to allow
2 development inside the production environment?

3 **A.** No. I think that's a case-by-case
4 determination based on, you know, what the
5 business needs in terms of development. And, you
6 know, one might seek to keep developers out of the
7 production environment.

8 There's no absolute in this case, and
9 there may be business-driven reasons to allow for
10 developers to work in the production environment.

11 **Q.** Do you agree that "SDL, secure
12 development lifecycle," is a term of art within
13 the cybersecurity field?

14 **A.** Yes. It's a term of art within the
15 cybersecurity field.

16 **Q.** And do you know which organization
17 invented or first documented the SDL?

18 **A.** You know, again, I'm not quite sure
19 why we're working on history at this point, but,
20 you know, I know that Microsoft had an early role
21 in, you know, the concept of secure -- you know,
22 secure software development.

23 **Q.** Do you recognize Microsoft as an
24 authority on the SDL process?

25 **A.** You know, there might -- you know, so

293

1 is, you know, part of what, you know, in my
2 practice, I'm looking for in this area, because
3 there's plenty of good guidance.

4 **Q.** Okay. Do you acknowledge that threat
5 modeling is a security best practice within an
6 SDL?

7 **A.** I would say threat modeling is
8 mentioned in, you know, that security -- you know,
9 secure software development, you know, practices,
10 yes.

11 **Q.** Okay. And do you agree that threat
12 modeling is a standard practice within the SDL?

13 **A.** You know --

14 **MR. TURNER:** Wait a minute. Wait a
15 minute. Within the SDL?

16 **MR. CARNEY:** Within an SDL.

17 **THE WITNESS:** So, yeah, we're saying,
18 sort of, conceptually if an organization is doing
19 software development and secure development, is
20 threat modeling a standard?

21 **BY MR. CARNEY:**

22 **Q.** Standard practice, right.

23 **A.** You know, I don't have the data. You
24 know, I guess if "standard" means, you know, some,
25 you know -- some high percentage of the

295

1 there are many authorities on -- you know, or
2 many, sort of, organizations that, you know,
3 provide advice around, you know, the conduct of
4 secure software development.

5 You know, that device is used by
6 teams, you know, in order to hopefully, you know,
7 improve security practice, you know, generally --
8 you know, as a sort of general perspective on
9 how -- how this works in the field.

10 **Q.** Have you ever read the book by Michael
11 Howard and Steve Lipner produced by Microsoft,
12 "The Security Development Lifecycle"?

13 **A.** I'm aware of the book, but I haven't
14 read it.

15 **Q.** Okay. Do you recognize that book as
16 an authority in the field?

17 **A.** As I said, I don't actually look to
18 find authoritative sources related to secure, you
19 know, software development.

20 Just, you know -- you know, practices
21 and procedures that are, you know, advised to
22 companies in pursuit of that -- you know, pursuit
23 of secure software development.

24 But you know, the issue of an
25 authoritative source is sort of not something that

294

1 organizations that do software development, you
2 know, use threat modeling, I actually don't know
3 whether that's a case, because there's some pretty
4 small organizations that do software development.

5 And, you know, they -- they -- my
6 sense is there's probably a lot of them that are
7 not doing threat modeling, so I wouldn't call it a
8 standard.

9 **Q.** Okay. Do you recall whether the
10 Microsoft SDL book has an entire chapter on threat
11 modeling?

12 **A.** I don't.

13 **Q.** Okay. Would it surprise you that it
14 does?

15 **A.** No, it would not.

16 **Q.** All right. Do you agree that
17 "penetration testing" is a term of art within the
18 cybersecurity field?

19 **A.** Yes.

20 **MR. TURNER:** I'm just going to object
21 to form.

22 **THE WITNESS:** Okay.

23 **MR. TURNER:** Go ahead.

24 **THE WITNESS:** I'm going too fast.
25 Yes.

296

Gregory Rattray
2/12/2025

1 BY MR. CARNEY:

2 **Q.** And what is penetration testing,
3 according to standard cybersecurity practices?

4 **A.** Again, the notion that, you know,
5 there's standard practice in cybersecurity is --
6 you know -- you know, often really not the case.
7 I mean, there are a lot of ways to conduct
8 penetration testing, so, you know, I don't know
9 that there's a standard way.

10 There are probably plenty of, you
11 know, people that depict how they think you should
12 do penetration testing.

13 But, you know, the notion of, you
14 know, from -- you know, looking at a -- a code --
15 like, an application or a network and seeing if it
16 can be -- in the case of penetration testing
17 intruded upon, I think that's what people think
18 about when they think about pen testing.

19 **Q.** Okay. If we could just quickly look
20 at paragraph 6 of your report --

21 **A.** Uh-huh.

22 **Q.** -- page 2 carrying over to page 3.

23 **A.** Repeat the location again?

24 **Q.** Sure.

25 It's page 2 to 3, paragraph 6 --

297

1 You know, generally, that's what I'm
2 referring to when I talk about structured testing.

3 **Q.** Okay. And what are the forms of
4 penetration testing that you recommend to your
5 clients?

6 **A.** Yeah, again, it -- it really is, you
7 know, situation dependent, yeah. It's very much
8 situation dependent.

9 **Q.** Based on the documents that you've
10 reviewed, how does SolarWinds perform penetration
11 testing?

12 **A.** You know, during their -- you know,
13 software development process, is it -- a series of
14 tools that are used, reports that are generated,
15 you know, related to penetration testing. I mean,
16 the FSRs in many cases document that.

17 **Q.** Are you aware of SolarWinds
18 conducting -- having any external penetration
19 testing conducted?

20 MR. TURNER: Objection to form.

21 External penetration testing of
22 software or external penetration testing of their
23 network?

24 BY MR. CARNEY:

25 **Q.** Of their software.

299

1 **A.** Uh-huh.

2 **Q.** -- the last sentence of paragraph 6,
3 you say, "My teams also assisted our clients in
4 conducting penetration testing in red team
5 exercises both of which involved structured
6 testing efforts to find flaws and vulnerabilities
7 in IT defenses."

8 **A.** Correct.

9 **Q.** What do you mean by "structured
10 testing efforts"?

11 **A.** You know, that -- you know, when we
12 conduct, you know, penetration testing or
13 network-based red teaming, that, you know, there
14 is a structure to our conduct of that activity in
15 terms of what -- what we will do, how -- how that
16 will interact with the client network, procedures
17 for, you know, starting the testing.

18 You know, notifying clients about the
19 fact that it's occurring. You know, procedures
20 for if their incident response team, you know,
21 detects the testing, you know, how to handle that.

22 You know, structure in terms of the
23 nature of the reporting that we would undergo, you
24 know, we would provide at the end of, kind of,
25 conducting either pen testing or red teaming.

298

1 **A.** You know, I didn't analyze, you know,
2 what -- I mean, yeah, I didn't analyze if they had
3 external, you know, penetration testing of -- of
4 software.

5 You know, again, they had a very
6 robust process for, you know, pen testing, you
7 know, in the -- you know, in the -- you know, the
8 evidence I examined and the -- also the -- the
9 leaders of SolarWinds testified that they were
10 doing it.

11 **Q.** All right. I could show you in your
12 report, but just tell me if this is wrong.

13 In paragraph 87, you say that,
14 "Penetration testing of software is often done
15 with the assistance of automated tools which can
16 simulate various types of attack -- attacks."

17 Is that true?

18 **A.** In paragraph 87, you know -- let's
19 see. Down in, like, paragraph -- paragraph (c),
20 okay. Let me just take a quick read.

21 (Pause for reading/reviewing.)

22 **A.** So I think you read a portion of this,
23 but maybe just restate.

24 **Q.** All right. So in paragraph 87,
25 subparagraph (c) --

300

Gregory Rattray
2/12/2025

<p>1 A. Uh-huh --</p> <p>2 Q. -- on page 48 --</p> <p>3 A. -- yes.</p> <p>4 Q. -- you say in the second sentence, "As</p> <p>5 with vulnerability testing, penetration testing of</p> <p>6 software is often done with the assistance of</p> <p>7 automated tools which can simulate various types</p> <p>8 of attack."</p> <p>9 A. Correct.</p> <p>10 Q. Are there any other penetration</p> <p>11 testing activities that -- other than those that</p> <p>12 use automated tools that you're familiar with?</p> <p>13 A. I mean, yes.</p> <p>14 Q. And what are they?</p> <p>15 A. You know, you could, you know, have --</p> <p>16 and I have seen, you know, this executed, you</p> <p>17 know, that the pen tester could just use -- and,</p> <p>18 again, maybe this is a nuance in terms of</p> <p>19 automated tools, but not pen testing tools, the</p> <p>20 normal ability of a computer to interact with</p> <p>21 another computer and see if they can gain access</p> <p>22 to the tested -- you know, either application or</p> <p>23 computer.</p> <p>24 So I wouldn't call that sort of</p> <p>25 activity automated tools.</p> <p style="text-align: center;">301</p>	<p>1 THE VIDEOGRAPHER: The time right now</p> <p>2 is 6:29 p.m.</p> <p>3 We are off the record.</p> <p>4 (Whereupon, a recess was taken at</p> <p>5 6:29 p.m.)</p> <p>6 THE VIDEOGRAPHER: The time right now</p> <p>7 is 6:36 p.m.</p> <p>8 We're back on the record.</p> <p>9 MR. CARNEY: All right. Dr. Rattray,</p> <p>10 I have no further questions at this time. I want</p> <p>11 to thank you for your time today.</p> <p>12 THE WITNESS: Thank you.</p> <p>13 MR. CARNEY: It was nice to meet you.</p> <p>14 EXAMINATION</p> <p>15 BY MR. TURNER:</p> <p>16 Q. Should be pretty brief.</p> <p>17 So, Dr. Rattray, let's pick up where</p> <p>18 Mr. Carney had left off a little while ago.</p> <p>19 He asked you about whether the terms</p> <p>20 "secure development lifecycle" is a term of art.</p> <p>21 Do you remember that?</p> <p>22 A. I do.</p> <p>23 Q. And he asked you about whether it</p> <p>24 comes from Microsoft.</p> <p>25 Do you remember that?</p> <p style="text-align: center;">303</p>
<p>1 Q. All right. And just a second ago when</p> <p>2 we were talking about paragraph 6 --</p> <p>3 A. Uh-huh.</p> <p>4 Q. -- and your team conducting</p> <p>5 penetration testing, which involves structured</p> <p>6 testing --</p> <p>7 A. Uh-huh.</p> <p>8 Q. -- efforts, I'm just trying to</p> <p>9 understand, what's the specific structure that you</p> <p>10 follow?</p> <p>11 A. As I talked about it, you know, the</p> <p>12 structure that I'm talking about there is</p> <p>13 structure around the process by which we do it.</p> <p>14 Mostly to ensure that the safety and -- of the</p> <p>15 client.</p> <p>16 Again, our penetration testing tends</p> <p>17 to be network penetration testing. We actually</p> <p>18 don't do application-level penetration testing,</p> <p>19 which is what, you know, is at issue in the</p> <p>20 SolarWinds case.</p> <p>21 MR. CARNEY: Okay. Could we take,</p> <p>22 like, two minutes.</p> <p>23 MR. TURNER: Sure.</p> <p>24 ///</p> <p>25 ///</p> <p style="text-align: center;">302</p>	<p>1 A. I do.</p> <p>2 Q. I think what Mr. Carney was getting</p> <p>3 at -- and correct me if I'm wrong -- is that if</p> <p>4 SolarWinds uses the phrase "our secured</p> <p>5 development life cycle" --</p> <p>6 A. Right.</p> <p>7 Q. -- in its security statement, would</p> <p>8 that be understood in the industry to mean that it</p> <p>9 does everything that Microsoft includes in its</p> <p>10 SDL?</p> <p>11 A. No, no.</p> <p>12 MR. CARNEY: Objection. Leading.</p> <p>13 BY MR. TURNER:</p> <p>14 Q. And why not?</p> <p>15 A. You know, "secure development</p> <p>16 lifecycle," you know, again, is a broad -- you</p> <p>17 know, broadly interpreted term. You know,</p> <p>18 generally means there are things that you should</p> <p>19 do in order to make sure security is baked into</p> <p>20 your software development.</p> <p>21 You know, the term at the level of</p> <p>22 secure development lifecycle is that broad, and</p> <p>23 you know -- you know, is not pinned to any</p> <p>24 specific, you know, set of practices.</p> <p>25 Q. And so in your experience, do</p> <p style="text-align: center;">304</p>

<p>1 companies tend to do software -- excuse me, secure 2 development lifecycle the same way, or do they 3 take different approaches? 4 A. Yeah. There's many different 5 approaches. 6 Q. And in your experience, is it possible 7 to have a secure development lifecycle without 8 having formal threat modeling? 9 A. Yes. You could say you're doing 10 secure development, you know, in a lifecycle 11 fashion without threat modeling. 12 Q. Your report in places relies on some 13 documents that date back before the relevant 14 period; is that right? 15 A. That's true. 16 Q. For example, I think we talked about 17 you cited a chat containing a screenshot of the 18 password policy settings from before the relevant 19 period? 20 A. That's right. 21 Q. Why, in your view, did you believe 22 that that was reliable evidence of SolarWinds's 23 practice during the relevant period? 24 A. You know, first, that screenshot is -- 25 you know, the type of direct evidence you're</p> <p>305</p>	<p>1 process -- 2 A. Uh-huh. 3 Q. -- this was from before the relevant 4 period, right? 5 A. That's correct. 6 Q. Why did you consider this to be 7 relevant evidence as to SolarWinds's practices 8 within the relevant period? 9 A. Again, we -- we know from this -- you 10 know, both, again, statements of executives and 11 the presence of artifacts in the relevant -- you 12 know, in the relevant period, like the final 13 security reviews, that, you know, the practices 14 outlined in that deck, which appears to be a 15 training deck, you know, extended, you know, into 16 the relevant period. 17 But that -- that particular deck shows 18 SolarWinds starting a process of doing Agile 19 development, and ensuring security is part of 20 their approach to Agile development. 21 Q. As early as -- 22 (Simultaneous unreportable crosstalk 23 occurs among parties.) 24 (Stenographer requests one speaker at a 25 time.)</p> <p>307</p>
<p>1 looking for just, in general, when you're doing 2 these sorts of assessments. 3 You know, they -- they say that 4 they're -- you know, conducting enforcement and, 5 you know, the mechanism by which they were doing 6 that is the use of active directory to enforce 7 strong passwords. 8 That particular artifact, you know, 9 shows that that -- that statement that, you know, 10 of how they were doing their practice is just 11 directly true. 12 It just shows the practice in 13 implementation. 14 You know, it also -- have evidence 15 to -- you know, that demonstrates that that 16 continued, you know, into the -- into the relevant 17 period, both in terms of, you know, testimony and 18 auditors also looking at that specific situation 19 and showing that that -- that implementation of 20 the -- you know, the password practices was in 21 place during the relevant period. 22 Q. And with respect to the training slide 23 that we looked at earlier -- 24 A. Yes. 25 Q. -- the SolarWinds development</p> <p>306</p>	<p>1 BY MR. TURNER: 2 Q. As early as 2015; is that right? 3 A. Yes. As earlier as 2015 and then, 4 again, evidenced during the relevant period in 5 execution of the things that were outlined that 6 had started as early as 2015. 7 Q. Let's go way back to sort of the 8 beginning of the deposition. 9 You were asked about whether you have 10 any certifications in various cybersecurity 11 areas -- 12 A. Yes, I remember being asked. 13 (Simultaneous unreportable crosstalk 14 occurs among parties.) 15 BY MR. TURNER: 16 Q. -- or from cybersecurity authorities. 17 Let me ask you: Are certifications 18 seen as important in the cybersecurity field, in 19 your experience? 20 MR. CARNEY: Objection. Vague. 21 THE WITNESS: You know, in general, 22 especially for the type of activity I was 23 conducting here in terms of, you know, assessments 24 of the presence of processes, you know, they're 25 not, you know, seen as sort of necessary or even</p> <p>308</p>

<p>1 sometimes particularly relevant to one's expertise 2 in order to conduct these processes. 3 BY MR. TURNER: 4 Q. And has any of your clients ever asked 5 you for certifications before engaging you to 6 conduct cybersecurity assessments? 7 A. No. 8 MR. TURNER: No further questions. 9 MR. CARNEY: Just one brief follow-up 10 question. 11 EXAMINATION 12 BY MR. CARNEY: 13 Q. Mr. Turner had asked you about your 14 reliance on evidence or documents from before the 15 relevant period. 16 Do you recall that? 17 A. Yes. 18 Q. Okay. And so, for instance, he 19 mentioned the slide deck relating to SDL. 20 Do you recall that? 21 A. I think -- I think it's development 22 process. You know, I mean, it was in our 23 discussion of SDL, but -- this slide deck -- 24 Q. Yeah. 25 A. -- is I believe what we were talking</p> <p>309</p>	<p>1 processes during the relevant period. 2 Q. And then actually just one more. 3 The folks that work for you at Next 4 Peak, that, for instance, do penetration testing, 5 did they have the certifications that Mr. Turner 6 was asking you about? 7 MR. TURNER: Object to form. 8 THE WITNESS: Yeah, for the pen 9 testers? 10 BY MR. CARNEY: 11 Q. Yes. 12 A. You know, I actually don't know 13 necessarily if they -- they have those 14 certifications or not. I mean, I'm -- yeah, I 15 don't know for certain whether they have them. 16 MR. CARNEY: All right. No further 17 questions, sir, thank you. 18 THE WITNESS: All right. 19 MR. TURNER: None for me. 20 THE VIDEOGRAPHER: The time right now 21 is 6:45 p.m. 22 We are off the record. 23 THE STENOGRAPHER: Mr. Turner, did you 24 want a rough draft? 25 MR. TURNER: Yes, please.</p> <p>311</p>
<p>1 about -- I was talking about with Mr. Turner. 2 Q. Okay. And the fact that you relied on 3 documents like the slide deck that predated the 4 relevant period, does that mean you were unable to 5 find equivalent documentation to that slide deck 6 from during the relevant period? 7 A. No. I mean, it does not mean that. 8 As I stated, the types of things that were, you 9 know, begun, you know, in training starting in, 10 you know, 2015 as outlined in this deck were 11 evidenced by, you know -- you know, processes like 12 we discussed at length like the final security 13 review, which was definitely prevalent throughout 14 the -- you know, the relevant period. 15 Q. But did you find an equivalent slide 16 deck from the relevant period? 17 A. I didn't -- I'm not sure even why I 18 would have looked for one. You know, the point 19 was -- you know, at least in my assessment was to 20 show that, you know, they had -- they had in 21 place, you know, during the relevant period per 22 the securities statement processes. 23 This deck shows they initiated those 24 processes and other evidence, you know, shows that 25 they -- you know, they were implementing those</p> <p>310</p>	<p>1 THE STENOGRAPHER: And regular 2 delivery on final? 3 MR. TURNER: Yeah, that's fine. 4 (Time noted: 6:46 p.m.) 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25</p> <p>312</p>

313

314

315

314

A			
A-1 95:14	135:12 136:4,20	281:7	allowed 42:8 149:20 175:2
A-2 83:15 85:24	accidentally 260:16 276:6	addressing 236:19 282:1	175:12
a.m 2:22 9:3,11 50:21,24	accomplish 151:4	adds 115:3,23	allowing 168:5 290:11
51:1 95:4,7,9	account 34:18 39:13 174:15	adjust 58:19	alpha 188:23
abilities 11:6	220:24 221:15 235:20	administrative 89:13,14,19	ambiguity 178:18
ability 48:21 53:4,8 216:6	accountant 72:3,22	ADMINISTRATOR 1:24	amended 165:10
301:20	accounting 72:5,11	advanced 82:1	Americas 2:20 3:19 9:13
able 11:10 20:4 80:15	accounts 90:11	advice 294:3	Amin 89:25 93:2
149:17 229:18 241:21	accuracy 94:3,16	advise 25:23 26:1 27:3 81:2	amount 12:12 54:25 62:16
245:11	accurate 84:2,3 93:6,13	82:24	82:12 169:9 287:23
absent 39:2	94:9 122:22 123:3,12	advised 26:5 294:21	analogous 23:23
absolute 293:8	153:12 181:24	advisor 25:16	analogy 230:11,22
absolutely 78:24 210:3	accurately 48:9 53:9	Affairs 45:17	analysis 81:10 139:21 140:2
abstract 271:20 272:2	achieve 32:7 256:15 259:16	affirm 180:20	156:1,7,8,25 157:13 178:5
abstracting 152:7	achieved 156:21	affirmed 9:22 159:1	206:23 207:7 212:7 232:22
abstractly 292:17	acknowledge 295:4	affront 260:9	232:24 233:11
accept 276:2 284:17	acknowledges 265:6	afternoon 61:14 138:17	analysts 45:5
acceptable 184:9 185:18	acquire 51:10	157:6	analyze 26:8 133:24 147:15
265:4,11,19,22 283:13,14	acronym 237:22	agencies 90:20	155:17,21 300:1,2
acceptance 281:17,20,24	act 248:23	agency 280:4	analyzed 26:19 147:16
283:4,6,9,15 284:2,3,15	acted 164:8	agenda 201:9	and/or 9:22 314:9,11
285:1,15	acting 279:5	Agile 198:7,11,23 199:16	Andesite 81:24 82:6,9,11,13
accepted 72:11 247:10	action 1:6 51:15,17 313:12	200:23 201:2,3 202:17,21	82:17,21 83:4 96:5
286:10,22 287:1	313:13	214:6,8,9,23 215:16	Andy 165:4,9
accepting 251:10	active 112:10 182:25 185:24	307:18,20	ANNIE 4:14
access 6:23 27:25 28:17,25	186:2,12,12,23 187:4	ago 126:21 196:6 214:1	answer 5:20 11:1 23:14
29:6,8 30:1,5 31:7 47:2,6	194:20 216:5 306:6	302:1 303:18	47:20 71:1 110:15 187:16
56:18 62:21 74:4 91:18	activities 25:15 36:16 37:6	agree 74:17,22 84:14 85:14	187:17 202:3 245:14
93:20 122:12,22 124:13,14	81:14 98:20 212:12,13	86:5 88:6 96:17 100:22,23	259:11 261:11 269:23
126:4,22 127:12,16 128:24	235:18 250:17 257:7 258:8	101:2,4 114:7,24 119:23	answer's 286:18
131:25 132:9,10,15,19,24	258:13 263:21 268:1	143:17 156:10 184:7	answered 47:21 80:4 169:3
133:7,13 134:3,10,25	281:13 301:11	185:16 186:15 189:3,7,20	242:24,25
135:9 136:17 137:4,10,23	activity 25:2 31:21,23 50:7	191:21 193:16 202:9	answers 11:5
139:8,23 140:12,13,14,23	81:10 151:2 246:11 252:13	217:22 218:12 222:18	Anytime 154:22
140:24,25 141:1,4,4,7,9,15	253:24 256:11 283:12	223:1 224:7,9 225:2	apart 59:24 290:4
141:17,23 142:1,10,13	291:2 298:14 301:25	226:13 227:13 237:23	APIs 287:15,18,19 288:10
143:3,16,20,24,24 144:18	308:22	240:4 247:3 261:2 270:18	Apologies 122:14
148:25 149:13,21 150:8,10	activity,' 252:10	271:9,13 273:5,12 274:11	app 240:16
157:11,22,23 158:10	actor 250:8	275:8,14 283:6 286:25	appear 147:21 159:15
164:16,24 165:10,13,16,24	actors 34:23 35:3 39:15	287:11,21 289:5 290:6,10	163:12 201:22 226:5
166:13,16 167:14,18,25	248:24 250:7	292:7,25 293:11 295:11	appeared 119:8
168:5,11,16,25 169:16,23	actual 18:3 58:14 188:17	296:16	appears 241:18 254:2
170:4,6,15 171:4,17 172:2	266:12	agreement 34:10 94:7	307:14
172:3,7,15,18,24 173:3,13	actuality 58:2	agreements 25:14 31:8	appendices 43:12,14 44:3,5
173:14,15,20,23,23 174:9	acumen 29:25	ahead 116:13 127:5 128:3,5	appendix 48:4 62:4,5,10
174:22,24 175:2,4,9,11	add 96:10 245:5	168:9 183:10 185:6 208:25	66:14
178:23 179:2,12,23 181:5	added 96:12 195:3	267:18 279:25 296:23	apple 291:4
181:22 188:19 194:19	addition 29:22 174:21 204:2	AI 81:24 96:5	applicable 81:13 193:6,13
216:18 219:25 220:2	additional 47:15 173:15	Air 17:8,10 28:9,12,15 29:1	193:13,14 195:14,21
241:21,23 257:13 282:5	Additionally 81:23	92:16	application 33:8 207:3
287:2,21,23 288:7 289:6	additive 115:16	al 9:14 73:9 315:3	240:16 244:12 297:15
289:12,17,23 301:21	address 58:20 195:10	aligned 77:4 106:13	301:22
accessed 135:5	281:25 292:2	alleged 53:23	application-level 302:18
accesses 133:3 134:18,19	addressed 196:8 210:15	allotments 201:16	applications 33:20,23 193:7
	addresses 90:9,10 174:18	allow 175:12 293:1,9	193:15 195:15,21 234:22

<p>applied 16:4,7 69:25 applies 196:3 263:18 apply 195:13 230:13 263:19 approach 6:14 39:25 71:21 76:8 100:1 104:5 140:6 142:15,23 150:8 212:23 235:17 245:20 307:20 approached 203:22 approaches 16:20 28:6 31:4 250:8 305:3,5 appropriate 139:22 178:23 202:10 207:21 213:23 214:13 215:3,8 appropriately 150:9,12 approval 207:22 Approved 286:16 approximately 204:7 architecture 21:5 245:1,12 245:19 area 12:17,19 39:21,21 133:5 215:19 277:6 295:2 areas 14:10 111:20 112:7 142:23 153:24 281:12 308:11 argue 292:19 arrangement 49:4 arrival 90:7 arrived 105:8,9 art 247:4,6,8 293:12,14 296:17 303:20 article 6:10,13 92:2,3,12,12 100:2,9 101:1,10,14,23 102:2,17 103:25 104:4,6 articles 51:23 articulate 195:18 articulation 244:13 artifact 137:8,19 176:20 177:2,5 306:8 artifacts 67:8 69:4 71:14 135:17 142:19 150:14 152:23 166:10 167:23 169:11 203:10,13 230:6 235:12 249:18 307:11 artificial 82:2 aside 45:2 52:19 59:20 107:12 111:1 125:3,3 166:3 292:23 asked 34:4 39:9 64:20 67:19 72:1 83:23 88:14,14,20,22 89:4 124:11 141:24 146:18 173:21 177:11 303:19,23 308:9,12 309:4,13 asking 23:22 40:11 52:2,3 54:5 75:1,4,8 84:18 102:8 102:10,12 136:2,13 156:12</p>	<p>219:4 238:6,17 273:17 276:23,23 278:18 284:9 289:16,19 291:10 311:6 asks 256:14 aspect 144:1 226:15 257:20 279:22 289:9,20 292:2 aspects 198:4 203:17 206:7 asserted 152:20 250:16 asserting 52:11 156:17 178:6 266:1 assertion 169:10 175:5 189:3,21 253:21 assertions 52:12 128:25 154:3 256:1,7 257:3 265:14,24 281:3 asserts 258:15 assess 26:25 67:13,19 68:11 71:23 110:7,21 111:13 112:24 113:6 114:4 115:18 116:21 136:15 152:19 158:24 assessed 38:3 75:9 111:25 120:17 156:2 246:6 assessing 67:3 68:18 70:1 76:9 111:2 112:4 144:12 184:8 185:17 186:16 196:14 243:4 258:15 assessment 16:16 29:5 37:19,23 38:6,19 40:21 67:22 69:9 70:5 71:6 74:10 74:14,18,23 75:2,2,13,16 76:23 77:4 96:22 111:24 125:11 136:23 137:20 140:7 150:21 158:9 166:12 178:19 214:11,25 229:22 230:8 232:13 233:8,19 244:11,16 257:16,20 258:1 258:2 282:13 283:21 310:19 assessments 26:11 29:4 33:14 37:13 66:25 67:1 70:12 71:17 76:25 77:1 109:22 111:17 112:11,12 126:1 150:19 213:18 243:17,21 257:12,13 306:2 308:23 309:6 assigned 25:17 44:15 assignment 98:7 152:17 164:5 assist 78:14 assistance 44:24 300:15 301:6 assistant 91:15 93:23 assistants 45:4,8 assisted 298:3</p>	<p>associated 139:6,12,19 144:9 150:2 162:7 163:2 169:7 173:9 202:22 209:17 211:23 Association 2:15 313:23 associations 98:18 assume 42:8 72:10 124:24 147:13 160:2,15 213:11 Assumes 181:7 assuming 251:12,24 assumption 151:1 252:3 attach 43:17 attache 261:24 attached 44:5 160:4,14,16 161:14,14 163:9,16,21,24 314:10 attachment 161:5 attachments 43:17 44:9 160:9,11 163:12 attack 101:11 300:16 301:8 attacker 273:18 attackers 273:6 attacks 300:16 attention 122:23 170:20 218:21 227:19 attorney 10:6 attune 35:1 audience 99:9 audit 41:10 112:11 auditing 41:18 auditor 41:9,11 auditors 41:20 130:10 137:3 138:2 141:19 144:19 306:18 audits 40:7,9,19,23 41:2,15 41:18 71:20 142:21 augment 44:17 August 93:4 222:14 Austin 133:21 135:14 Authentication 220:21 Authentication/Authoriza... 188:20 193:5 authoritative 59:3 294:18,25 authorities 294:1 308:16 authority 293:24 294:16 Authorization 220:22 authorized 220:23 221:14 authors 232:12 233:19 automated 173:2,7 194:21 300:15 301:7,12,19,25 automatically 191:8 192:13 192:17 194:10 automation 134:13 195:6 available 37:24 71:16 209:10 276:6</p>	<p>Avenue 2:20 3:19 4:7 9:13 avoid 170:3 avoiding 262:22 aware 22:21 36:3 50:5,7 88:7,11 91:16 99:4 218:19 248:16 272:9 294:13 299:17 awareness 97:11</p> <hr/> <p style="text-align: center;">B</p> <hr/> <p>B 87:9 88:6 201:2 bachelor 13:7,9 back 39:7 42:20 51:2 57:6 62:4 79:11 94:13 95:10 109:21 134:19 136:5,13 138:15 166:7 182:18 183:19 190:14 206:23 212:3 220:13 221:25 224:25 228:8 271:5 303:8 305:13 308:7 background 27:24 45:11 backtrack 72:1 backup 232:23 233:12 236:5 backwards 160:5 bad 263:1 badly 278:20 baked 37:1 304:19 ballpark 60:13,14 bar 190:10 barely 252:9 base 143:9 214:24 based 34:7 53:5 76:23 98:2 105:18,25 106:6 107:24 112:25 115:18 116:22 126:16,24 127:1,15 132:24 219:5 293:4 299:9 baseline 214:21 basically 21:2 25:14 34:15 39:12 57:5 108:19 109:13 115:6 117:12 119:8 127:9 127:21 136:24 161:3 168:12 172:6 208:21 255:5 259:15 basics 199:16 basis 52:5 109:8 143:5 158:8 167:21 168:6 169:24 175:3 187:3 214:24 230:20 233:24 Bates 131:15,19 160:21 161:23,25 171:23 172:9,10 177:2 200:2 205:13 217:19 232:8 237:15 285:14 bathroom 182:6 Baynard 4:6 161:7,11,25 163:1</p>
--	--	---	--

bearing 75:15 BECKY 4:15 beginning 89:3 234:3 252:9 308:8 begins 200:2 begun 310:9 behalf 3:3,15 4:3 90:16 behave 34:24 35:3 behavior 283:13 believe 11:21 22:8,20 44:16 48:11 49:8 50:11 52:21 53:1 66:6 68:22 71:22 84:3 91:14 96:13 116:2,2 121:18 126:13 145:22 153:16,25 161:7 164:1 165:12 169:4 186:22 209:6 210:3 224:14 244:20 246:15,20,23 252:1,24,25 282:3 288:17 291:5 305:21 309:25 benchmark 265:3 BERKOWITZ 4:5 best 11:6 53:8 117:5 188:21 191:6 192:18,18 194:8 195:7,23 196:3 201:4 227:14,17 248:17 292:8,17 292:21 295:5 better 279:16 beyond 110:24 127:18 144:24 291:11 big 43:19 60:13 285:19 bigger 42:4 billed 60:10,19,21 billing 216:18 282:5,6,7 286:3 binary 37:19 biscuit 260:18,19 264:7 bit 23:10 27:20,22 37:12 49:3 97:1 129:1 145:17 150:21 156:2 157:6 183:24 184:1 186:7 197:24 247:2 271:8 BizApps 286:2 block 229:8 230:11 Bloomberg 92:2,22 board 82:24 bodies 22:3 body 112:19 126:15 bold 93:19 book 294:10,13,15 296:10 bottom 145:18,21 146:3 147:21 148:12,12 175:19 208:12 218:7 264:12 282:25 BOUND 8:8	brain 38:25 breach 6:12 90:6,16 92:14 100:16 104:3 272:6,13 275:9,13 breached 91:19 breaches 90:5 101:25 271:14 break 10:22 11:2 24:8 50:15 50:17 72:2 83:19 95:1 101:2 122:3,6 131:5 135:20 137:6 138:11,18 182:5 201:18 227:9,24 233:6 247:1 270:21 290:4 breakdown 237:22 breaks 10:21 brief 111:23,23 303:16 309:9 briefcase 260:20,21,22 261:25 262:21 264:3,6,9 briefly 47:25 77:7 bringing 238:12 broad 87:11 234:4 235:18 240:1 249:12 304:16,22 broader 29:9 83:23 88:15,20 88:23 248:14 broadly 27:13 35:11 40:17 107:19 235:6 238:11 248:22 250:9 304:17 broke 51:4 138:24 228:11 broken 212:18 Brown 1:8 46:18 52:6,14 65:9,12 66:1,9 183:2 286:11,22 Brown's 286:16 BRUCKMANN 3:7 budget 83:13 87:21,21,24 88:2,9 94:21 budgeting 74:15 bug 199:17 build 104:5 building 6:13 99:25 200:19 built 93:17 121:20 200:24 bullet 218:8 bullets 86:16 Bush 92:19 business 90:11 100:25,25 113:7 114:5 126:10,18 166:11 293:5 business-driven 293:9 buying 170:13 bypassing 275:15	300:19,25 C-e-r-t 22:19 C-I-S-S-P 22:12 C-o-m-p-T-I-A 21:14 calculate 265:19 268:19 calculated 266:9,11 268:11 268:12 calculating 268:2 California 2:8,13 313:22 call 28:20 33:16,18 62:17 64:12 66:9,9,11 69:12 91:3 91:3 103:19 111:10 204:13 242:8 250:10 296:7 301:24 call-out 39:5 40:1 called 9:22 25:25 26:4 28:3 28:4 83:21 91:17 93:24 99:25 102:25 103:1,12 105:18 107:25 124:15 139:25 142:3,7 244:14 246:24 callout 35:12 281:5 callouts 240:13 calls 111:10 118:7 121:12 135:9 242:20 256:10 capability 18:12 19:16 20:16 capital 22:19 41:15 198:20 caps 21:22 40:5 237:4 capstone 206:19 care 98:4,10 102:9,13 career 28:2 Carney 3:5 5:5,7 10:2,6 12:1 12:9 16:23 18:2,17 19:14 20:1,12 29:20 30:15 32:9 32:19 40:13 41:1,13 42:3 42:13 43:19,21,24 44:1 45:1 46:13,14 47:24 49:11 49:24 50:1,16,19 51:3 52:18 53:18,20 55:11 56:6 57:13 58:1 63:6,16 64:1,24 72:13 73:2 74:1 75:4,7 76:16 80:12 84:20,22,24 91:5,24 94:24 95:11 98:11 99:6,20 102:6,12,15 103:7 103:12,15,18,23 108:6 109:1 110:5,18 111:15 116:14 118:24 119:3 122:5 122:8,10 123:15 127:20 128:16 131:2,8 132:6,12 132:14 134:1,23 135:22 136:1 138:6,16 144:6 147:3 148:9 154:11,18 157:16 159:3,7 160:6,10 160:18,19 161:16,17,22 162:3,5 163:13,22 165:15 166:1 168:20 169:22	171:15 176:25 177:6 180:22 182:1,7,19 183:15 184:15,20,24 185:4,7,14 185:15 189:13,22 193:22 194:5 195:9 199:23 203:1 205:8 208:13 209:11 211:6 214:10 216:12 217:7 219:1 219:15 223:4 225:13 226:21 227:8,12,23 228:9 232:1 237:11 239:17 240:3 240:24 241:10,12 243:11 244:23 247:9 249:5 251:14 252:5 254:10 255:12 257:1 259:3 260:7 261:10 262:8 262:9,13,17 264:17,20 266:21,22 267:1,20 270:19 271:6,22 272:20 273:13,21 274:1,19 275:22 279:21 280:12,19 282:24 283:2 285:11 287:6,10 288:11,19 290:3,18 291:12,19 292:18 295:16,21 297:1 299:24 302:21 303:9,13,18 304:2 304:12 308:20 309:9,12 311:10,16 Carneyc@sec.gov 3:13 carries 264:8,13 carry 80:24 carrying 262:21 297:22 case 11:14 12:11,14,17,20 23:20 25:3 26:8 44:15 47:11 49:6,13 50:3,6,10 51:6,7 52:5 56:1 59:18,20 59:25 60:2,7,16 67:12,18 68:1,4,5,14 69:2,15,20,22 69:23 70:11 71:12,12 75:20 103:16 114:16 130:13,20 133:19 138:19 148:21 151:21 152:8,12 153:7,25 157:10 164:6 169:21 170:8 174:11 179:19 180:15 185:22 186:4,20,22 187:1 196:16 205:2,3 209:22 215:15 216:2 225:11 236:11 238:4 239:16 249:3,17 250:12 251:16 281:18 282:14 283:25 284:8 293:8 296:3 297:6,16 302:20 315:3 case-by-case 293:3 cases 26:13 28:12 48:13 57:11 65:14 68:22 99:13 111:23 124:25 130:22 142:21 150:5 263:16 281:1 299:16
--	--	---	---

category 266:13 causality 66:18 cause 235:14 313:4 caveat 119:24 120:4,24 121:17 caveats 120:5 CCR-NJ 1:23 313:24 CCR-WA 1:24 313:25 CCRR 1:23 cell 287:11 CEO 82:24 certain 16:20 30:5 54:21 67:4,13 80:14,25 111:19 112:7 133:2 140:5 283:8 311:15 certainly 24:18 25:10 31:6 32:13 67:25 253:20 260:2 264:2 266:4 269:15 CERTIFICATE 5:12 313:1 314:1 certification 21:9,11,23 22:12,15 72:5 certifications 21:8,17 22:7 22:16 80:14 81:1,4,7,12 308:10,17 309:5 311:5,14 certified 1:22 2:7,8,9,11,12 2:14,15 72:4 313:22,22 certify 22:4 313:2,10 314:6 CertNexus 22:18 chain 7:12 217:17 challenging 53:3 chance 264:16 change 44:8 55:14 57:14 132:4,18 133:12 155:24 156:19 158:2 162:19 164:16,24 165:11,13 315:4 315:6,7,9,10,12,13,15,16 315:18,19,21,22 changed 87:9 132:22 133:15 changes 117:1 155:4 159:13 162:22,23 164:7 165:2 314:9,11,14 chapter 296:10 characterization 127:7 194:1 characterize 26:17 characterizes 31:11 characters 188:23 chat 176:11 183:2,4,16,20 184:3,10,14,21,23,25 185:23 215:6,9 305:17 chat-type 230:8 chats 185:19 check 175:15 224:13 245:22	288:17 checking 175:13 checklist 235:10 checkmark 208:19 209:6,25 210:1,4 checkmarks 208:2 209:15 Chicago 4:8 chief 25:16 81:23 82:23 83:9 83:15 84:5 85:11,24 86:9 86:17 89:12,14,15,19 91:10 92:19 93:7,24 94:17 96:4,9,15 107:2 224:15 choice 288:3 choose 62:24 63:11,11 choosing 124:20 chose 126:16 223:23 Chris 10:6 50:13 122:2 154:9 185:6,10 222:7 224:3,20 225:19 228:17 273:18 282:23 290:13 Chris's 225:24 CHRISTOPHER 3:5,7 chronological 218:5 circumstances 55:6 222:12 222:19 223:2 CISO 17:4,24 23:25 33:25 83:21,22 84:1,10,13,15 86:6,13,21 87:2,22 88:2,16 88:24 89:1,2,9 90:1,3 96:19 107:2 citation 245:5 cite 100:24 126:14 131:13 160:23 171:16 232:5 237:5 237:6,14 239:5,10 259:21 cited 61:3 62:22 66:14 77:3 124:18 149:8 160:22 172:4 175:23 205:5 232:4 236:4 241:8 285:16 305:17 cites 73:7 74:7 75:20 231:11 233:8 citing 160:2 161:21 Civil 1:6 185:8 clarification 78:23 132:13 133:12 162:4 197:7 256:14 clarify 24:1 115:23 123:13 144:8 161:20 185:2 clarifying 132:8 184:17 classic 248:5 clause 187:9 193:20 clean 10:18 174:5,12 cleaning 174:16 clear 133:19 144:15 149:5 151:6 156:4 162:21 163:4 165:23 176:11 182:23 209:21 210:9 221:9 225:14	227:3 229:7,7 269:21 270:8,13 clearly 105:22 118:5 130:6 137:24 140:7 148:23 150:7 151:21 152:21 157:9 162:16 173:6 174:10 202:7 244:14,21 263:1 clicked 172:6 client 298:16 302:15 clients 78:15 79:11 298:3,18 299:5 309:4 close 24:16 83:5 coach 229:7,12 coaching 185:4 code 18:13 276:5 297:14 coder 18:16 30:12 32:17 79:4 coding 18:3,5,16,19 19:9,11 30:13 32:18,18 cofounded 77:17 cofounder 95:16,22,25 COLE 4:20 collaboration 44:24 collect 82:8 Colquitt 251:24 254:7,20 Colquitt's 200:18 202:19 250:22 251:6,9 252:16 253:3 254:1 Columbia 45:14 Column 286:9,20 287:13 Columns 286:15 come 49:5 57:6 63:12 274:25 comes 303:24 commander 28:11,15 92:16 commands 17:7 commencing 2:22 comment 46:25 156:24 216:9 commenting 25:6 comments 46:6,9,21 213:22 215:14 Commission 1:4 3:4 53:23 common 142:15 170:5 284:3 commonly 155:6,9,18 156:10,18 158:4 communicate 64:14 communicating 53:7 communications 46:3 65:1 companies 12:20 16:15,25 17:1,13 23:23 24:22 25:5,9 26:6,12 27:14 33:1,2 34:25 40:22 52:22 100:13,17 101:5 111:13 113:16,19	114:8 118:7 120:24 137:1 137:2 170:5 294:22 305:1 companies' 101:24 157:22 company 26:1,20 27:4 33:9 34:17 35:1 36:21 38:2,10 54:20 56:1,12,12 57:16,20 58:21 59:4 67:4,5,19 70:6 75:23 76:4 77:17 81:25 82:25 88:15 90:4 97:12,22 101:13,19,21 104:1 111:3 111:24 112:21 114:13,20 114:22 115:11 126:11 128:12 133:10 158:19 170:12 181:6 184:9 185:18 186:17 193:12 202:12 243:5 257:22 284:16 company's 23:2,12 98:23 102:13 214:3 216:10 compare 117:16 compensate 271:10 275:7 compensating 275:2,12 278:2,23 279:8,15 281:5 286:20 complete 14:17 15:6,10 314:7 completed 124:2 completely 58:3 73:19 184:16 266:15 complex 53:3 57:17,21 58:23 188:22 191:7 194:9 196:4 233:1 complexity 30:6 182:25 186:4,14 191:9 192:11 194:11,22 compliance 106:24 107:2,4 107:10,13 111:10 compliant 109:23 110:1 111:3,6 complicated 20:11 149:24 163:12 comprehensive 29:16 174:17 CompTIA 21:13 Compton 89:17,23 computer 13:6,8,13,16 14:13,15,22 15:10,18,22 136:15,15,16,19 137:16 301:20,21,23 concentration 14:4,9 concept 39:22 195:12 243:18 250:9 265:22 293:21 conception 240:1 249:12 conceptualization 215:19 conceptualizations 247:19
--	---	--	---

conceptually 295:18 concern 158:19 concerning 210:15,21 concerns 37:1 101:15 241:15 242:23 249:2 conclude 128:23 concluded 129:14 concluding 2:22 conclusion 129:24 conclusions 52:4 126:25 175:1 conduct 29:3 76:24 79:2 80:11,15 81:8,16 125:10 145:1 149:22 151:2 166:12 246:11 255:6 294:3 297:7 298:12,14 309:2,6 conducted 26:11 34:14 39:10 66:24 71:18 74:14 78:21 79:1,25 125:14 150:18 156:7 172:18,21 173:18 214:8 240:7 249:10 299:19 conducting 64:3 67:21 70:5 78:15 81:5 252:19 258:8 291:2,7 298:4,25 299:18 302:4 306:4 308:23 conducts 71:6 258:14 confidence 174:8 confident 135:18 149:19 168:19 181:23 confidential 7:16 confirm 42:19 209:24 282:3 confirmation 173:16 confirming 174:23 conflicts 90:20,23 91:4 Confluence 198:19 conform 254:24 confused 160:1 conjunction 33:8 41:2 281:18 connected 313:12 connection 279:17 consequences 278:16 279:1 280:15 consequential 261:9 consider 12:17 13:2 39:18 66:13 209:2 238:20 247:25 307:6 consideration 245:2 274:25 considerations 236:20 238:13 239:25 considered 37:3,5 62:7 274:17 285:1 considering 36:25 consistent 129:15 187:12	187:23 188:10 243:20 consistently 130:14 Consortium 21:24 constant 106:21 227:19 constantly 279:5 constituted 58:17 constitutes 207:19 265:17 consultant 17:12 29:2 consulted 59:23 consulting 24:5 25:13 26:14 32:23 33:10 41:19 45:5,18 77:17 contacted 49:7 contain 120:24 208:17 283:21 contained 216:4 276:5 containing 305:17 content 127:1,23 128:14,18 128:19,20 contents 201:10,12 context 23:4,6 59:2 146:14 158:19 166:7,11 171:9 175:20 176:4,9 177:14 183:8 189:19 191:3,4,15 199:9 203:15 213:23 216:24 222:24 223:6,12,19 225:21 229:25 230:3,24 254:3,5,5,6,8 263:16 271:19 278:19 284:22 288:8 contexts 284:6 contextual 198:15 271:12 contextually 166:25 198:15 266:15 continue 97:24 185:13 continued 59:9 184:6 186:22 306:16 continues 215:13 contractor 165:11,17 contractors 165:20 contractual 11:24 control 12:21 18:6,25 26:12 26:24 27:25 28:17 32:7 34:25 38:7,7 41:20 111:20 112:7,9 124:15 125:12 127:16 134:10 137:5,23 141:15,19,23 157:11 165:23 173:23 179:2,24 223:10 226:25 259:20 260:5 261:18,18,23 263:3 267:4,14 268:8,15 269:17 272:12 278:23 279:8,9 286:20 controlling 170:7 controls 12:22 15:22 18:4,7	18:12,13,15,22,23 28:25 29:6,9 30:1,5,14 31:2,7 40:24 41:4 47:2,6 56:19 62:18 64:6,11 67:4,6,9,13 67:20 68:19 74:5 111:19 119:19 122:13,22 128:24 137:10 140:23,25 141:4,7 141:10 142:10,22 143:3,20 144:4 166:13,17 167:14,18 167:25 168:25 187:11,23 188:19 190:6 227:1 257:7 257:14,23 258:24 259:8 261:5 263:10,14 265:5,12 268:4,5,6 272:16,21,24 273:4 274:17 275:1,2,6,12 278:1,2 279:16 281:5 conventions 31:5 conversation 46:23 65:12 66:1 181:10 242:12 274:24 conversations 63:5,8 64:19 65:3,4,8,20,24 66:1,5 COO 91:17 cool 122:6 copy 42:5 48:5 119:6 154:12 254:14 Corp 1:7 9:14 93:3 315:3 Corporation 25:17 correct 13:19,21 14:1 48:14 60:1 65:10 67:17 78:9,12 82:7 86:3,4 89:4,21 90:2 90:17 105:4,7 112:15 158:11 183:22 193:19 196:7 241:20 253:9 282:12 282:19 298:8 301:9 304:3 307:5 314:7 corrected 43:6 corrections 43:8 314:9,12 314:13 correctly 113:8 136:7 152:5 corresponding 155:5,25 159:14 160:4,14 Council 92:18 counsel 9:16 46:3,5 61:18 61:22,24 62:24 63:5 64:7 64:19 66:9,11 108:20 313:14 counsel's 133:11 211:7 count 124:7 counted 146:23 204:24 countries 33:1,1 couple 40:2,4 48:13 95:13 122:24 123:17 130:22 131:4 227:8 course 14:12,23 15:13,15 15:17,23,23 16:1,2 48:24	62:15 127:9 146:15 154:22 176:5 213:13,13 234:6 courses 13:12,14,16 14:14 14:15,17,19,20,25 15:6,10 16:4,6 court 1:1 2:9,12,16 9:18 10:13 11:5 29:18 42:15 48:18,20 313:23,23 cover 55:8,8 covered 46:4 211:4 covers 25:23 193:6 195:14 292:20 CPA 72:23 create 105:17 151:19 152:2 152:4 210:7 created 19:6,9 124:16 199:1 creating 18:4 creation 24:13,19 credentials 273:6 credit 15:24 criteria 126:17 critical 257:25 cross-check 175:10 crosstalk 102:20 123:5 163:17 231:20 267:5 270:4 290:15 307:22 308:13 CRR 1:23 crux 153:20,21 cryptography 16:4,7 CSF 107:24 113:2,5 114:3 120:11,18 CSR-CA 1:24 313:25 CSR-TX 1:23 313:24 Cummings 89:24 current 44:18 47:22 70:19 currently 77:15 218:9,9 customers 33:22 CV 27:22 43:15 48:5 77:10 77:12,20 78:10 82:4 83:15 83:25 85:23 86:5,12,15 95:14 cyber 6:14 13:24 28:4 67:20 83:10,11,17,24 84:6,9,11 84:16,25 85:3,12,13,25 86:10,17,22 87:5 88:21 89:5,10,11 91:15 92:17 93:18,24 94:18,19 96:17 99:15 100:1 104:2,6 105:18,23,25 106:2,3,24 107:14,20,22 cyberattack 100:15 cybersecurity 13:1,3 16:10 16:14 17:2,3,5,8,14,20 18:4 21:7,16 22:3,6 26:12 27:20 28:4,13,21 35:6,14
---	--	--	---

36:11 37:13,16 39:19 45:16 51:14 52:20,23 53:3 54:21 58:7 59:24 66:25 67:20 70:6 73:19 75:24 76:1,5,13,20 77:16 82:1 88:2,9 90:15 93:2,12 97:17 98:4,15,23 99:8 101:5,24 102:13 104:9,18 105:2,12 105:19 106:1,7,14 107:4 107:20,21 108:3,5,9,13 109:9,24 110:8,22 111:3 111:14 112:1 113:1,7 114:5,14 115:20 116:3,7 116:18,24 117:5,18 118:2 119:18 120:16,18 121:6,9 121:15 122:1,1 184:8 185:17 186:16 202:11 213:17 214:12 219:5 227:14 243:4,15,21 247:4 247:11,14,20 248:6,11,17 254:25 256:13 257:23 258:1,22,24 259:6,8,14 261:5 265:7 278:6 280:13 292:7 293:13,15 296:18 297:3,5 308:10,16,18 309:6 cycle 304:5 D D.C 2:17 3:11 damage 275:10,12 Dana 89:24 Danny 4:19 9:8 data 6:12 30:7 46:25 47:1 62:17 65:18 79:10 82:1 90:5 91:19 92:14 100:24 124:15 125:8 130:9,10,24 141:22 142:11 143:3 147:18 167:19 169:9 173:1 173:6,22 174:9,12 175:14 208:19 209:20 216:18 241:14 242:23 268:5 269:3 287:3,18 289:7,12,18 295:23 database 161:13 167:19 database's 143:4 databases 193:7,15 195:15 195:22 date 9:10 42:21 69:12 162:2 286:21 305:13 315:2 dated 6:6,8,17 314:19 315:25 dates 209:6 Daubert 48:25 day 69:17 188:5 222:7	223:17,22 224:3,5,20 225:19 228:21 229:12,18 234:6 313:16 314:19 Day's 222:18 228:18 DB 286:3 deal 43:19 278:2 dealing 104:2 284:3 Deasy 89:24 December 6:17 42:21 43:3 decided 80:8 96:9 114:13 124:23 224:3 deciding 30:4 decision 32:5 108:18 decisions 283:18 deck 7:8 199:15 200:11,21 201:24 202:7,15 307:14,15 307:17 309:19,23 310:3,5 310:10,16,23 decks 202:10 DECLARATION 5:13 declarations 23:11 114:9 declare 314:3 declared 99:17 decommissioning 181:5 deemed 283:12 deep 80:10 125:23 137:21 156:4 173:5 203:21 deeper 55:7 138:4 deeply 107:23 225:8 defendant 68:14 defendants 1:9 3:15 4:3 68:7,8 defending 28:24 defense 6:14 61:22 83:11 84:9,11,16,25 85:3,13 94:19 100:1 defenses 78:18 298:7 define 23:9 28:2 35:7 54:11 defined 36:16 40:17 57:2 153:8 178:2 200:13 Defining 21:9 definitely 38:15 49:9 64:13 156:20 218:11,13 310:13 definition 21:10 degree 13:5,8,17 14:18 15:7 15:11 38:5 45:15 69:11 70:13 130:5 Delaware 2:18 delays 91:18 94:1 deliberating 25:5 deliverables 222:13 delivered 229:14 delivery 312:2 delve 27:19 Demarest 91:12,13,16 93:23	demonstrate 143:18 151:25 166:15 167:23 168:4,23 demonstrated 139:24 142:3 150:7 203:21 demonstrates 246:2 306:15 demonstrating 100:17 denominator 267:2,7 268:2 269:3,4 270:15 denominators 269:19 dependent 266:16 267:14 280:18 299:7,8 depict 297:11 depicted 145:1 184:14 depicting 189:25 deploy 19:16,23,24 20:16,22 20:24 21:1 32:6 deployed 20:2,9,11 32:3 188:24 deployment 21:3 deploys 19:12 deponent 9:15 deposed 232:13 deposition 9:12 10:7 60:23 61:6,11,19,23,25 138:20 138:22 141:13 144:15 185:5 200:18 251:1,18 253:1 254:7 308:8 313:5,6 314:5,13,14 315:2 depositions 71:13 134:8 142:17 150:17 202:20 derived 106:23 describe 26:24 35:11 36:14 49:5 90:8 183:3 203:9 described 31:24 66:21 67:14 73:8 74:8,12 75:6,10 88:14 108:19 111:8 112:6 134:7 137:8 163:1 211:20 254:25 describes 29:1 78:7 describing 58:6 description 6:4 7:4 8:4 27:1 185:11 descriptions 135:13 235:7 design 17:1,13 18:9,9 81:9 112:24 116:21 236:20,21 236:22 237:5,19,25 238:7 238:13 239:6,14,24 241:4 241:14 242:3,4,7,14,22 244:25 245:2,12,18 designed 16:10,13,21 17:3 17:9,20 67:7 115:18 121:19,21 designing 30:1 80:6 desk 175:22 despite 261:2	detail 110:9 114:15 133:1 141:14 147:15 153:3,5 209:9 282:14 detailed 28:17 65:15 105:14 135:16 153:22 209:12 235:7 details 46:12,15 58:16 87:12 110:6,20,23 detect 119:19 detects 275:9 298:21 determination 37:20 58:15 58:18 79:10 257:10 281:23 293:4 determinations 41:3,10 206:10 269:18 determine 38:20 57:10 136:20 180:12 181:23 266:6 determined 215:3,8 determining 38:4 57:7 75:23 76:3,19 267:15,15 develop 32:6 292:12 developed 32:3 107:18 198:14 developer 216:18 developers 33:8 240:7 282:5 287:2 288:9 289:6 289:11 290:6 291:1,3,17 293:6,10 developing 32:11 33:16 236:8 development 7:7 28:5 31:7 32:16,21,24,25 33:3,6,11 33:14 34:17 35:4 37:2 197:20,25 198:5,12,23 202:8 203:11,16,23 206:11 207:1 212:11 214:9,25 222:12,19 223:2 225:16 226:3,18 227:4 235:20 236:7 238:20 242:9 249:3 249:4,17 280:5 282:9 288:13 289:2,7,13,24 290:7,12,24 291:7 292:12 293:1,2,5,12,22 294:4,12 294:19,23 295:9,19,19 296:1,4 299:13 303:20 304:5,15,20,22 305:2,7,10 306:25 307:19,20 309:21 develops 33:19 deviation 125:21 device 273:2 294:5 devices 19:2 devine 269:2 dialogue 178:22,25 difference 70:25 71:3
---	---	---	--

<p>165:16 190:13 248:1,8 different 12:25 17:7,9 22:3 30:23 33:1,2,23 36:19 39:23 76:12 77:2,23 81:12 81:13,14,14 94:25 98:19 106:11,11 115:1 116:19 126:10,10 133:9,9 135:13 189:8,11,11,14 202:3 218:10,23 219:17 247:18 248:13 262:18 265:21 268:24 279:24 280:11 284:6 291:1 305:3,4 difficult 230:2 259:15 digital 113:13,17,20 119:25 278:23 279:10,12,23 digitally 280:10 diligencing 197:8 Diplomacy 14:7 Diplomate 2:8 313:21 direct 73:14 84:11 85:3,12 89:12 122:23 155:14 170:19 185:23 305:25 directed 83:11 84:9,25 85:17 94:19 direction 82:25 83:2 directive 117:15 directly 11:18,25 32:8 65:1 65:7 135:12 161:21 306:11 director 84:14 86:1 91:15 93:24 directory 182:25 185:25 186:2,12,13,23 187:4 194:21 216:6 306:6 directs 84:16 dirty 74:15 disagree 117:7 223:24 disclaimer 52:9 disclose 87:10,11 discovery 137:15 276:17 discuss 65:12 91:18 93:25 94:1 171:3 216:17 249:25 258:10 264:19 discussed 32:3 59:18 71:19 79:4 80:9 94:15 106:20 107:8,14 124:11 157:5 163:7 216:2 221:13 234:5 235:15 248:21 277:2 310:12 discusses 258:11,13 281:1 discussing 118:20 162:9 186:3 188:4 212:6 213:5 216:25 223:18 231:10 232:3 235:23 242:1 251:9 261:16 discussion 154:15 168:13</p>	<p>200:16 203:15 234:2 250:22 289:14 309:23 discussions 61:4 91:2 100:3 106:21 138:19 disinterested 313:8 dissertation 13:23 distant 178:14 distinct 195:17 distinction 70:18 261:14 distinctly 92:9 distributing 280:9 distribution 133:6 280:8 DISTRICT 1:1,2 distro- 134:17 division 93:24 133:21 Doberman 7:19 Doctor 20:23 22:21 112:13 131:9 138:17 142:25 159:8 162:6 185:16 240:25 document 8:5 42:23,24 86:4 99:22 118:22 119:10 128:22 137:11 151:20 152:3,5 154:16 161:5 164:20 174:4 189:25 198:25 199:14 200:25 201:6 208:15,19,23 214:20 217:24 231:10,12,17 232:3 232:5,7,20 233:16 237:6 237:14 238:1 239:4,5,8,11 239:13 240:6 241:8 243:6 285:14 299:16 documentary 156:5 214:18 documentation 61:3 64:5 65:7,16,18 144:17 152:23 174:4,25 179:16 211:19 212:19 221:21,24 236:10 243:7,20 246:16,18 283:11 283:17 310:5 documented 214:2 293:17 documenting 216:3 252:13 253:6,24 documents 43:14 62:22,25 63:9,14,18 64:8,21,23 65:2 65:6 66:20 73:7,12,13,24 73:24 75:5 124:22 127:1 129:12 151:23,24,25 156:4 159:23 160:23 161:4 163:5 176:16 179:11 186:17 198:19 206:4 208:16 211:4 211:8,9,12 213:22 215:14 231:15 235:25 236:22,22 237:5,19,25 238:7 239:7 240:8 241:3,13,19,22,24 242:3,4,14,21 243:1 244:2 299:9 305:13 309:14 310:3</p>	<p>doing 25:9 26:10,20 38:19 38:22 39:25 56:18,20 57:5 57:11 59:6,8,12,13 79:19 108:8 120:19 127:19 128:10 129:25 135:19 137:25 151:8 156:6 157:10 158:14 183:7 223:22 236:7 240:21 244:15,22 252:10 252:11 253:4,23 265:20 281:15 282:9 289:13 295:18 296:7 300:10 305:9 306:1,5,10 307:18 domains 64:21 doubt 128:11 Dr 10:3 42:14 51:4 91:25 95:12 99:21 119:4 182:20 205:9 228:10 254:22 271:7 303:9,17 draft 25:6 46:22 311:24 drafter 100:7 drafting 25:7 46:12,16 drafts 46:6 dramatically 272:24 draw 175:2 driven 284:22 drop-off 58:17 dropping 116:25 drops 100:14 duly 313:3 duties 85:22</p> <hr/> <p style="text-align: center;">E</p> <hr/> <p>E 3:1,1 4:1,1,12,12,17,17 earlier 31:13 43:8 62:22,23 67:21 69:7,11,17 70:7 97:1 97:4 141:25 146:18 161:8 186:21 215:7 226:8 289:15 306:23 308:3 early 81:24 105:8 186:10 207:13 293:20 307:21 308:2,6 easier 199:6 285:3 easily 166:14 167:23 168:3 easy 227:18 education 48:10 effect 177:12 effectively 69:16 271:16 272:8 effort 99:17 105:16 106:12 106:16 180:18 211:25 efforts 78:17 97:16 106:15 108:3 151:25 275:16 298:6 298:10 302:8 eight 124:8,8,20 126:13 128:19 131:13 133:25</p>	<p>139:10 either 35:16 36:9 38:3 39:6 227:3 241:21,24 298:25 301:22 electronically 161:4 element 31:3 33:11 126:4,22 169:7,8 202:23 206:9 207:9 214:15 225:19 238:18,20 239:2 247:23 248:14 289:10 292:1 elements 204:1 223:25 244:16 elevated 157:25 email 3:13,22 4:10 7:12 58:22 59:3 90:10 148:11 148:13 161:6 174:18 216:3 216:5,24 217:17 218:3,7 221:18 222:1,5,25 223:6,8 223:21 224:4 225:22,24 226:18 228:14,18,24 229:1 229:11,15 230:8 250:22,25 251:6,10,17,19 252:17 253:10 254:2,2,5,13,14,18 emails 73:13 213:19 229:17 229:21,25 230:6 emphasis 33:6 employ 76:21 employed 70:6 75:24 76:20 employee 45:18,19 59:18 131:24 132:15 134:3,25 147:11,13 149:14 165:9,11 165:17 218:10,24 219:18 269:1 employee's 180:25 employees 93:10 124:1 158:1 165:21 184:10 185:19 221:4,11 employees' 213:19 employing 76:4 employment 179:7,14 180:4 empty 238:3,5 240:5 enable 106:23 108:5 encouragement 230:20 ends 191:19 218:1 enforce 182:24 188:22 191:7 192:14,18 194:9 195:25 196:4 306:6 enforced 191:8 194:10 195:7 257:23 enforcement 58:12,17 90:20 192:11 195:5,24 306:4 enforcing 58:3 engaged 97:13,13 engagements 24:6 41:19 engaging 309:5</p>
--	--	--	---

engineering 13:13,16 232:23 233:12 engineers 210:13,20 ensure 67:9 302:14 ensuring 32:15,21 106:19 107:7 108:12 307:19 entail 235:4 enterprise 19:12 20:3,9,17 21:6 32:4 enterprises 12:21 19:10 entire 17:25 18:10 42:23,24 55:22 56:19 58:25 133:6 157:14 180:10 191:13 254:18 286:6 296:10 314:4 entitled 92:12 entry 77:21 78:11 environment 12:21 32:25 108:23 226:4 227:5 282:10 289:25 290:8,12 291:3,8 291:18 292:13 293:2,7,10 environments 33:14 127:17 143:4 167:20 289:3 290:25 equity 82:12 101:20 equivalent 310:5,15 Eric 4:20 183:2 Errata 5:14 314:10 315:1 error 158:21 259:22 260:9 262:24 263:22 265:4,11,19 265:23 266:8 268:2,10,19 269:12 errors 38:22 158:20 259:24 265:6 266:24 267:9 269:25 escalate 273:7,19 especially 98:17 100:13 173:4 240:20 308:22 ESQ 3:5,6,7,8,9,17,18 4:5,6 establish 106:13 206:5,6 established 25:1 104:18 105:2 establishing 187:10 establishment 24:13 26:5 estimation 76:14 110:10 126:3 274:23 et 9:14 73:9 315:3 evaluate 152:18 evaluated 142:24 evaluating 143:25 257:6,17 evaluation 7:16 111:22 127:11 event 263:1 282:7 evidence 36:22,25 37:10,24 44:17 64:11 71:8,23 73:14 93:23 112:9 124:12,13 125:1 126:1 129:5 130:23 137:21 144:4,14,20 154:1	155:14,19 156:5 162:10 164:3 168:15 177:12,25 178:3 181:8,21 182:23 185:21,23 186:1,5 187:10 200:17 202:16,19,24 203:25 204:2,3,13,16 209:21 212:14 214:18 234:7,14,23 236:18 242:16 244:20 252:21 253:3 263:13 279:4 300:8 305:22 305:25 306:14 307:7 309:14 310:24 evidenced 234:13 308:4 310:11 evidencing 124:2 145:14 155:5 evidentiary 187:3 evolution 14:21 evolved 272:13 evolving 272:19 exact 87:9 153:3 174:1 253:18 exactly 12:5 24:17 25:20 98:9 110:3 116:20 150:1 177:22 201:14 233:15 291:22 examination 1:14 2:3 5:1,4 10:1 126:2 303:14 309:11 examine 139:11 188:6 examined 9:23 57:12 139:13 170:17,18 202:24 300:8 examining 127:13 example 17:18 20:13 21:12 74:7 75:19 114:22 142:11 149:4 164:12 179:15 239:17 259:21 270:16 285:4 305:16 examples 124:8,18 125:2 144:10 149:6 Exchange 1:4 3:4 53:22 excluded 48:18 exclusion 126:20 excuse 110:12 122:25 219:8 256:9 305:1 execute 39:23 executed 125:18 126:5,23 128:11 138:2 144:16 212:21 301:16 executing 155:12 execution 80:7 125:22 128:14 130:5 134:15 150:24 180:1 256:25 308:5 executive 93:2 executives 137:2 307:10 exercise 74:16 80:11,25	81:6,16 158:23 250:2 exercised 82:16 215:2,7 exercises 78:16 79:3,7,24 80:1,6,15 298:5 exhibit 6:5,7,10,13,15,17,19 6:21,23 7:5,7,9,12,15,18 7:21 8:5 41:23 42:1,11,18 43:13 44:5,12,20 47:12 48:1,5 53:11,17,17,18 62:3 66:13,14,23 77:9,10,20 78:3 83:14 91:22 92:1 95:14 99:18,22 104:14 119:1,5 120:7 122:14 131:5,6,11,15 138:25 139:11 140:16 141:3 143:7 145:7 146:6,8 147:1,8 154:10,17 159:5,9 166:22 166:23 170:21 171:11,21 176:23 177:1 182:21 188:14 190:15 199:21,25 205:6,10 207:25 210:20 213:2 217:2,15 220:14 221:22,22 223:14 228:11 231:1,24 232:7 233:10 235:22,23 237:9,13 240:22 241:3,8 264:13 277:4 285:9,13,25 288:20 exhibits 6:1 7:1 8:1,8 42:16 48:2 exist 81:15 137:17 204:3 210:8 212:18 235:14 existed 14:25 127:10 174:21 234:8 255:23 existence 126:24 150:6,11 150:14 209:20 234:19 exit 34:10 expect 36:22 118:13 121:13 145:3 172:11 244:8 246:4 249:9 281:15 expectation 170:10 255:10 265:16 expected 156:8 265:3 experience 21:3 26:17 29:1 30:13,19 31:12 32:1,11 35:5 36:20 37:13,14 40:8 40:12,14,17 41:14 48:10 76:24 77:1 79:21 98:2,3 111:2 214:12 219:6 284:24 304:25 305:6 308:19 experienced 90:6 experiences 35:10 41:16 111:13 expert 6:5,7 11:14 13:3 35:6 44:20 48:12,17,21,24 49:6 67:3 68:1,13,15,24 92:17	103:6 104:13,14 117:12 121:14 153:20,21,22 181:15 231:2 271:24 expertise 12:17,19,24 27:20 27:25 72:6,17,22 79:22 309:1 explain 161:1 168:2 explained 76:7 103:10 180:7 254:6 explaining 199:16 explanation 250:25 251:11 252:16 explanations 177:16 explicitly 111:9 exposed 90:9,12 expressed 101:23 extended 307:15 extensive 172:7 extent 26:23 59:1 64:9 126:18 174:6 234:12 255:22 external 33:21 276:12 299:18,21,22 300:3
F			
F 3:10 face 234:18 251:11 283:22 284:16 facing 129:18 fact 73:23 75:10 88:1 89:25 127:10 135:15 136:24 139:22 141:18 142:20 173:13 178:17 179:20 194:20 203:19 218:23 219:17 221:14 223:13 234:23 238:6 244:13 259:16 271:10 274:9 277:11,17 279:2,3 281:7 298:19 310:2 factors 267:15 facts 181:7 factual 59:8 fail 272:24 failed 254:11 279:16 failure 261:22 fair 36:16,18 44:2 54:13 58:19 85:8 86:20 87:13,17 90:8,14,18 120:22 137:11 153:6,19 156:25 178:12 180:2 193:23 208:8 239:12 252:15 254:22 255:13,17 255:20,24 256:5,9 257:19 257:21 268:9 276:2 282:10 fairly 14:21 29:15 35:11 fairness 271:23			

<p>fall 62:20 falls 246:11 false 53:24 54:7 56:10 57:2 57:8 falsehood 54:12 familiar 21:13,21 22:18 35:21 36:1,5,10 46:18 51:20 67:1 172:13 301:12 familiarity 51:5 familiarize 217:10 far 12:11 39:8 48:8 57:19 163:14 FAS 236:21 237:4,19,20,24 239:6 240:8 242:2,13 fashion 74:15 146:21 207:5 305:11 fast 278:10 296:24 FBI 91:15,17 FBI's 93:24 feasibility 192:22 feasible 191:10,20,22 192:4 192:6,9 193:17,21 194:12 194:13 195:2,8,12,25 196:2,2 feature 237:24 242:7 features 216:11 236:23 February 1:16 2:21 6:3 7:3 8:3 9:3,10 313:16 314:8 315:2 federal 90:20 94:12 103:8 103:19 185:8 FedRAMP 74:10,23 75:1,9 feeding 35:2 feel 149:2 150:4 166:9 174:7 181:23 242:24 254:11 266:9 felt 125:16 174:2 210:8 215:23 field 12:23 15:20 22:4 39:19 51:12 53:3 130:15,18 133:24 147:18 248:10,11 278:6,9 293:13,15 294:9 294:16 296:18 308:18 fielder 259:23 fields 149:18 173:5,5 174:14 figure 93:14 129:5 178:23 filed 48:25 50:6 filled 123:25 130:15 164:23 177:23 178:7 final 7:9,18,21 203:5,9,20 204:20 212:13 239:24 243:18 307:12 310:12 312:2 finance 133:21 135:14 financial 89:7 99:14 100:13</p>	<p>106:17 112:21 114:22 227:1 financially 41:4 find 72:23 78:17 115:15 129:5 135:17 154:16 234:14 252:22 294:18 298:6 310:5,15 finding 253:14 276:4 findings 130:12 fine 42:6 213:12 312:3 finish 10:17 167:1 finished 44:14 Finn 7:22 firewall 47:7,8 firm 11:17 44:25 45:5 105:24 107:3 firms 98:5 108:1 first 17:18 28:20 65:11 69:24 71:2 80:13 84:7 92:6 92:11 104:18 105:2 115:17 115:24 116:8,18 117:1 119:16 123:1 124:9 128:8 130:4 131:16,17 132:9 140:24 147:10,10,19 148:6 148:6 159:20 164:13 167:10 171:23 176:11,19 191:18 199:13 205:11 208:10,12 213:20 218:8 220:22 224:25 237:2,17,25 238:9,10 239:4 241:3 253:25 288:24 293:17 305:24 fiscal 112:22 fit 55:15 114:20 117:14 118:8 214:23 five 88:10 flag 29:17 122:2 130:19 flagged 30:9 flaw 258:23 259:7,13,16,24 flaws 78:17 259:25 298:6 Fletcher 13:25 14:3,6,6,13 flip 159:21 198:16 focus 40:23 44:12 45:16 69:14,17 86:23 167:15 194:23 251:4 252:6 focused 6:13 61:11,25 73:23 81:25 99:25 104:5 153:24 199:2 focusing 178:15 179:4 fold 12:24 folks 311:3 follow 37:17,20,21 38:10 55:18 57:19 76:5,22 105:11 107:13 198:6 302:10</p>	<p>follow-through 245:24 follow-up 309:9 follow-ups 6:24 95:13 followed 34:7 55:19,21 57:17 76:19 106:19 107:8 108:4 109:10 142:8 143:9 143:19 151:12 155:6,10,18 155:19 156:11,11,18 157:2 157:23,25 163:1 198:22 206:6 following 37:15 38:13 54:21 54:24 56:13 100:15 101:11 158:3,4 186:2 200:13 202:12 280:23 follows 9:23 119:17 football 264:6,10 footnote 113:10,11,19 124:5 126:14 131:14 139:1 145:21 146:19,24 147:5,6 159:16,25 160:2,7,12,22 160:24 162:8 171:16,24 172:4 199:13,15 200:1 204:25 205:12 209:18 210:25 211:5,13 217:18 232:4 237:6,14 241:4,9 Force 17:8 28:9,12,15 29:1 92:16 Force's 17:10 foregoing 314:5 forensic 137:16 forensics 280:10 forget 51:15 forgive 25:23 form 16:11 17:23 18:14 19:7 19:18 20:5 24:3 30:2 31:17 32:12 40:10 41:7 44:21 52:7 55:3,23 56:23 57:24 63:2,20 64:18 70:9 72:9,25 73:21 74:25 76:6 80:2 90:25 98:6,25 99:10 102:1 107:16 108:15 109:25 111:5 116:12 127:3,6 128:4 129:7 130:2 132:3 133:1,19 134:2,5,7,17,19 134:20,21 135:6,10,12 136:5,12,21 137:12 143:21 144:23 145:25 147:17,18 157:3 158:5 161:9,14 163:6 168:7 169:2,14 177:17,18,22 178:7 180:6 184:12 185:11 189:10,17 193:18,25 194:15 202:13 208:24 214:4 215:11 218:15 219:7 222:21 225:4 226:11 240:9 243:8,23</p>	<p>247:5 248:19 254:9 255:2 258:25 259:9 261:7 271:17 272:10 273:9 274:14 275:19 279:19 280:16 283:10,16,21 285:16 287:24 288:15 291:9 292:14 296:21 299:20 311:7 formal 14:23 15:23,23 81:18 81:20,21 94:7 250:1 305:8 formalistic 235:1,3 249:24 250:4 formalized 232:14 233:20 234:17 formally 96:10 format 171:22 172:12 former 92:16 93:2 forming 214:14 251:5 forms 124:13 133:25 140:13 145:12 147:15 149:23 160:14,16 161:12 173:13 281:18,21 283:4,7,9 284:2 284:15,25 299:3 formula 266:23 formulation 17:5 forth 47:11 66:12 forward 122:24 123:18 198:16 200:7 283:14 found 73:12 118:22 150:19 210:15,22 230:6 234:18 foundation 99:1,11 133:17 137:13 165:18 200:19,20 200:23 218:16 225:5 255:3 foundational 200:22 215:18 four 208:7 fourth 213:17 frame 23:13 87:25 framework 104:9,18 105:2 105:12,17,19 106:1,3,7,13 106:19,22 107:7,11,14,21 107:23 108:4,9,14,21 109:9,14,15,24 110:8,22 111:4,8,14 112:2 113:1,23 114:14,17 115:8,10,20 116:4,7,18,24 117:5 118:2 118:6 119:18 121:6,11 framework's 117:18 frameworks 36:11 76:11 77:2 Fraser 147:22 148:2,13,17 fraudulent 52:13 free 166:9 frequent 255:19 261:3 frequently 269:16 friend 195:10</p>
--	---	--	--

front 118:1 120:3 188:13 193:1 220:16 250:13 frustrated 93:22 FSR 205:12,15 206:5 210:4 211:24 212:5,18 234:23 238:23,25 239:1 240:12,18 242:10,15,18 245:16,25 246:1,21,25 FSRs 203:9 204:7 206:9 210:12 211:22 214:19 234:21 236:3,18,19 238:6 238:15 239:10,21,22 242:5 244:4,5,14,25 245:8,10 246:5,10,10,16,18,21 253:15 299:16 full 28:23 37:23 47:19 56:13 155:17,17,21 176:3 181:20 191:15,15 199:9 200:6,17 202:19 215:16,22 281:13 fully 11:10 125:18 271:10 fundamentally 39:2 178:15 180:17 181:17 further 161:14 245:1 303:10 309:8 311:16 313:10 future 13:24 43:17	George 92:19 getting 63:4 66:19 106:10 110:6,20 125:12 132:9 249:15 267:19 304:2 GitHub 276:7 give 11:5 21:12 54:14,15 87:8 97:20 154:8 190:15 197:14 205:25 260:14 264:15 267:22 268:14 given 114:13 129:7 132:16 134:3,4 135:1,6,7 139:22 149:14 170:4 191:4 207:3 209:7 223:21 238:22 240:5 256:12 261:23 267:4 268:16 283:22 284:17 314:8 global 83:10,16,24 84:6 85:12,25 86:10,16,22 87:5 88:21 89:5,10,11 93:18 94:18 96:16 105:23 216:9 globally 89:6 GMFC 113:16,22 120:8 go 30:13,22 55:7 88:14,14 94:4,10 100:18 101:6 105:15 116:6,13 124:19 127:5 128:3,5 134:20 136:14,18,19 137:19 138:4 144:22 147:9 160:25 164:11 168:9 178:5 182:6 183:3,9,10 185:6 200:7 208:25 216:20 217:23 231:7 233:14,18 242:9 266:13 267:15,18 268:1,3 268:16 279:25 296:23 308:7 goal 255:10 goes 59:10 110:24 141:14 170:25 194:18 262:22 268:7 going 10:16 26:15 27:21 42:10 46:10 48:7 50:14 62:3 102:18,24 103:21 105:14 109:20 122:11 133:20 135:21 147:8 171:6 179:18 182:2,3,9,13 183:6 187:15 191:1,12 197:13 203:4 204:23 210:10 217:4 229:12,18 252:9,12 253:6 261:6 269:5 271:7 283:14 296:20,24 gonna 103:4 136:5,14 181:10 205:16 216:24 224:13 264:18,19 292:19 292:19 good 10:3,4 27:11 38:19	53:5 122:3,4 138:17 174:7 174:25 180:15 183:13 214:21 229:1,11 231:23 259:19 270:17 295:3 Gotcha 78:4 gotten 163:8 176:13 177:9 178:2,11 governance 120:16 121:9 122:1 government 94:12 260:16 261:4 gradation 39:4 Gradillas 9:9 graduate 45:14 Graff 76:22 118:22 175:23 214:17 231:11 232:4 233:7 254:2,11 265:2,10,13 266:1,8 268:10 280:25 Graff's 61:2 73:5 213:6 277:16 285:16 grammar 275:18 granted 158:1 granular 153:2 granularity 174:7 grave 261:20 262:25 GRAVELLE 4:14 great 44:11 77:14 113:20 217:13 219:2 229:21 Greg 92:16 170:23 Gregory 1:15 2:4 5:2,11 6:2 6:5,7 7:2 8:2 9:15,21 313:3 314:3,16 315:2 grew 93:22 ground 10:10 group 45:18 109:2 163:20 GSEC 22:15 guarding 261:25 guess 23:7 24:15 36:13 63:17 70:17 76:17 78:22 82:19 108:7 121:3 218:22 247:25 249:6 295:24 guidance 108:1,5,10,14 186:3 193:12 198:19 295:3 guide 108:3,3,22 113:6 114:4 115:14 120:19 121:9 206:25 guided 14:19 15:19 207:4,4 guys 131:3	handed 42:14 43:13 91:25 99:21 119:4 131:10 159:8 177:1 199:24 205:9 217:14 232:6 237:13 240:25 241:7 285:13 handle 170:6 298:21 handled 94:5 hands-on 19:21 happen 227:21 235:14 246:25 259:25 271:15 276:1 280:15 happened 163:4 183:24 184:1 263:9 278:19 281:25 282:1 happening 224:2 228:21 230:2 happens 261:1 263:24 269:16 272:6 274:2 happy 43:16,18 hard 30:6 178:22 Harvard 100:24,25 head 83:9,16,24 84:6 85:25 86:10,16,21 87:5 88:21 89:5,9,11 91:14 94:17 96:16 105:23 224:15 heading 93:20 100:12 122:20 123:10 239:11,13 242:2,3 243:18 headings 236:20 238:25 239:11 244:1 hear 161:10 219:9 heard 162:14 274:24 heavily 108:22 heavy 151:3 held 9:12 50:12 154:15 Helen 45:9 Hello 222:10 help 45:3,22,24 100:12 101:17 104:5 113:6 114:4 119:19 175:20,22 205:14 253:11 helped 17:4,12 281:25 helpful 48:2 helping 111:13,23 helps 27:21 148:16 hereunto 313:15 hesitant 87:8 137:18 hide 231:15 high 153:6 208:20 209:3 277:22 295:25 high-level 236:21 237:5,19 237:24 239:6 242:3,13 higher 89:9,15 highlight 229:5 highlighted 173:24 222:10
--	--	---	--

<p>225:15,19,22,25 highly 135:18 272:25 280:3 hired 11:18,21 124:1 166:11 history 13:10 293:19 hit 242:19 hold 13:5,7,8 21:7,19 22:9 22:17 72:4 95:19 96:6 256:23,23 holding 190:9 hood 38:12 hopefully 180:11 188:13 269:22 275:5 294:6 hour 50:14 60:8 182:10 270:20 hourly 60:6 hours 12:13 60:10,18,20 61:23 62:1 House 17:6 households 90:11 Howard 294:11 humans 38:21 227:17 hundred 204:22 hundreds 93:11,14 hypothetical 54:15,16 55:6 55:15 56:17,22 57:14,20 58:20 136:9 151:13 157:18 157:21 158:18 170:1,4 258:19 259:19 260:14,15 262:18,19 263:7,8 264:1 hypothetically 38:9 129:23 263:17</p> <hr/> <p style="text-align: center;">I</p> <p>I-S-C 21:22 i.e 120:17 ICANN 25:17 idea 24:25 34:15 39:12 231:23 identification 30:18,20 31:3 31:10,15,20 41:24 42:2 91:23 99:19 119:2 131:7 147:2 159:6 171:12 176:24 199:22 205:7 212:15 217:3 218:18 231:25 235:19 237:10 240:23 247:22 248:2,3,23 250:14 285:10 identified 31:9 204:25 225:10 236:24 258:17 265:10 283:7 identify 39:14 113:6 114:4 119:19 205:12 265:3 284:25 identifying 34:21 236:8 249:1 identity 186:25</p>	<p>IDs 220:24 221:8,15 Illinois 4:8 illuminate 177:21 179:20 190:5 242:5 illuminating 215:17 illumination 212:9 illustrating 215:24 illustration 178:14 201:4 illustrative 125:1 179:17 images 137:16 imagine 198:13 immediate 275:15 immediately 222:11 225:23 225:25 277:12,19 impacts 222:13 imperative 229:4 implement 12:22 28:10,14 34:5 135:13 151:20 152:1 152:3,5 153:2 216:7 implementation 17:22 18:1 29:14,24 30:9,14 31:2,20 38:21 64:6 69:5 71:15 107:3 112:10 125:13 134:21 137:22 141:7 143:11 149:3 151:24 152:10,24 153:3 155:15 162:18 165:1 169:14,18 173:25 179:1 180:13 186:14 188:9 204:2,4,17 204:18,19 206:16 209:21 240:15 242:16 244:11 245:23 255:6 256:16 265:5 265:12 269:17 306:13,19 implementations 30:11 238:24 implemented 67:9 70:2 140:12,25 141:4,10,15 142:18 152:16 180:19 187:11,22 202:21 240:21 implementing 31:15 35:16 130:12 149:1 162:21,22 178:25 310:25 implements 134:7 implication 130:9 290:23 implications 236:23 241:4 241:14 242:4,23 imply 113:3 114:1,18 115:11 important 10:15 11:3 52:21 128:8 251:16 261:12 278:6 308:18 imposed 48:20 impossible 259:15 improper 103:15 152:10 184:16 185:7 improperly 152:16</p>	<p>improve 294:7 improvement 81:25 inaccurate 85:9 153:10 inadequate 271:11 incident 51:21 91:21 94:5 100:18 101:6 218:11,13,18 218:25 219:6,10,18,20 223:17,20 224:11 226:16 230:18 260:2 263:5 271:10 271:16 272:7 274:9 275:9 275:13 276:3,11 277:11,18 278:4 279:11,17,23 280:2 280:13 281:8 282:1,2,4 284:1 298:20 incidents 119:20 268:3 277:17 281:2,22 include 28:22,25 113:25 128:23 188:23 189:4 191:22 244:25 269:18 included 15:21 18:6 120:25 189:8 210:12 214:7,7 239:24 240:12 245:17 includes 77:1 86:15 206:22 244:7 245:17 248:4 304:9 including 17:9 18:1 40:18 108:20 199:16 200:17 201:18 204:18 207:16 209:15 281:6 inconsistency 129:6 131:1 inconsistent 128:24 289:7 incorporate 46:8 incorporated 37:6 incorrect 176:12 incorrectly 58:6 increase 88:8 increasing 134:13 187:4 increasingly 186:12,13 independent 116:16 253:3 253:21 independent-guided 16:1 index 5:1 6:1 7:1 8:1 99:15 105:18,25 106:4 INDEXED 5:9 indicate 125:17 198:22 258:23 259:7 261:4 indicated 44:8 140:8 148:23 152:24 154:3 157:9 158:13 186:6 212:16 314:10 indicates 135:11 136:5 174:10 180:18 244:21 indicating 176:16 179:13 232:20 indication 261:22 indications 263:2 indicative 249:15 262:3</p>	<p>indiscernible 161:9 165:4 individual 25:2 108:25 133:13 150:23 168:22 181:13 individual's 53:8 individuals 52:22 109:3,4 indulge 131:4 industries 106:15 industry 75:22 89:6 97:16 98:17 105:24 106:10,12,17 140:9 142:15 212:23 230:4 235:16 245:21 304:8 industry-driven 105:17 industrywide 105:16 info 148:1 inform 98:22 99:5 information 5:17 12:21 13:1 14:17,22,23 15:21 16:19 21:23 28:3,14,16 29:3,10 40:24 53:6 67:5 68:11 69:1 83:9,16 84:5 85:11,24 86:9 86:18 89:16 92:17,20 93:8 94:8,17 96:16 97:21 118:17 121:22 141:1,5 157:8 158:13 173:24 193:6 193:14 195:14,21 220:5 221:3 224:15 225:9 226:24 informed 26:13 107:22 informing 249:4 infrastructure 21:5 inherent 81:16 inherently 265:15 initial 53:25 132:18 223:8 initially 19:9 28:3 93:17 initiated 310:23 inside 14:9 16:21 33:7 34:11 215:20,21 280:5 291:3,7 292:12 293:2 instance 27:9 98:3,13 118:19 157:14 226:14 227:7 238:22 257:22 258:23 259:7 261:21 287:5 287:7 309:18 311:4 instance-by-instance 153:4 instances 38:15 40:4 134:12 140:8 202:10 267:8 268:22 institute 35:22 36:2 106:5 107:14 116:23 Institute's 107:23 institutes 106:3 112:25 115:19 INSTRUCTED 5:20 Insulet 68:1,4,5,9,16,17 69:3 69:23 integrated 199:3</p>
--	--	---	---

intelligence 17:15 82:2 280:4 intended 239:20 intent 242:14 interact 298:16 301:20 interaction 269:8 interactions 94:11,11 interested 63:15 101:24 102:4 313:11 internal 33:21 58:22 92:21 international 13:20 14:3,4 21:22 36:2 45:17 Internet 25:17 interpret 121:5 149:17 interpretation 85:20,21 121:11 interpretations 247:15 interpreted 304:17 interpreting 120:25 interrupts 110:11 interview 254:19 interviewing 111:18 interviews 71:11 intruded 280:4 297:17 invented 293:17 invest 98:5 investigation 51:18 281:6 investors 98:4,10,23 99:5 101:18 invoices 12:4,7 60:12 involve 18:16,18,19,20 78:16 213:18 265:15 involved 18:4 19:11 24:12 24:19 25:4,12,20 28:5 30:4 30:24 31:6 32:8 33:3,13 51:7 79:9 97:15 98:19 108:20 157:25 198:4 207:21 249:20 257:16 298:5 involvement 32:11 34:1 40:13,14 197:25 involves 22:22 81:8 282:4 302:5 IPAM 7:21 ipMonitor 7:19 ISC2 22:1,6 ISO 36:1 isolated 141:22 278:3 isolation 143:25 issue 23:19 64:22 70:2 74:19,24 76:9 85:20 103:1 141:12 153:25 210:24 212:15 216:17 226:10 261:4,8,15 294:24 302:19 issued 269:1	issues 59:24 210:15,21 227:6 229:6 265:15 item 222:11 225:22,25 items 75:9 266:13 itself,' 252:11 <hr/> J <hr/> J 286:15 January 54:2,19 55:19 57:18 67:15 200:14 Jersey 2:9 JESSICA 2:5 313:21 Jessie 1:23 9:18 Jim 89:24 JIRA 210:14 211:18,23 212:1,5,17 JIRA-based 211:19 job 1:25 57:3 93:7 135:13 288:9,9 jobs 82:5 JOHN 3:6 joined 93:3 joining 98:17 Joseph 91:11,13,16 93:23 JPMC 100:15 JPMorgan 6:10 17:18 20:17 23:25 25:11 29:8 33:5,16 33:19 34:1,6,11,11 40:19 41:17 84:19 85:1,4 87:10 88:8 89:8 90:1,4,7,16 91:18 92:13 93:3 97:15 98:3,12,14 99:8 101:10 105:6,9,9,11,13,16 106:19 107:6,13,19 108:8 109:22 110:3,21 111:1 198:1,6 JPMorgan's 88:2 92:19 93:11 110:24 JPMorganChase 17:4 83:10 83:21 84:20 86:1 91:10 94:12,18 judge 265:4,11 judging 181:20 judgment 127:15 169:21 215:2,8 260:4 277:20 judgments 283:12 284:20 July 7:17 285:15 June 92:2,8,21 199:2 <hr/> K <hr/> K 286:15,15 keep 185:3 293:6 KEPES 4:21 keyword 64:16 Khadija 131:25 136:3 137:9 Killed 43:22	kind 20:19 33:15 48:20 126:7 170:3 272:1 298:24 Kline 65:9 66:2 knew 52:14 91:9 know 10:10,10,23 11:20,23 11:23 12:10,12,13,20,25 14:8,10 15:21,25 16:15,16 16:17,19 17:7,10 18:5,7,7 18:8,20 19:2,3,8,22 20:7,8 20:10 21:2,3,4 22:4 23:6,7 23:9,12,24 24:6,6,13,16,20 25:1,2,10,13,18 26:3,4,14 26:16,23,24,25,25 27:7,8 27:13,23 28:1,2,3,5,5,6,9,9 28:22,22 29:2,3,3,9,13 30:3,4,4,6,8,21,23 31:1,2,4 31:7,8,9,21,22,25 32:2,2,4 32:14,14,17,24,25 33:6,7 33:10,11,19,20,21,22 34:3 34:4,7,16,18,19,20,21,23 35:1,3,5,8,10,11,12,14,15 35:20 36:8,11,24,25 37:2,3 37:4,5,6,7,8,9,18,20,22,22 38:1,1,3,4,5,5,6,7,15,15,16 38:20,22,24,25 39:4,6,20 39:24 40:16,18,20,22,23 41:10,11,17,20 44:16,23 44:23,24 45:10 46:24 47:6 47:7,13,21 48:9 49:4,15,17 49:21 50:3,7 51:12,12,13 51:17,18 52:8,10,11,12,14 52:16 53:2,2,4,5,5,7,8 54:10,11 55:4,4,6,7 56:2,3 56:10,14 57:1,1,2,4,4 58:9 58:9,13,15 59:1,2,4,5,7,7 59:12,14 60:18,20 61:2,15 61:24 62:14,14,18,22 64:3 64:4,5,5,9,12,12 65:16,17 65:17 68:9,10,21,22,24,25 69:10,11,13 70:10,11,13 70:14 71:3,5,6,7,8,9,9,14 71:17,17,21 73:11,12,14 73:22,23 74:9 75:12,14,14 75:14,19 76:11,11,13,13 76:23,24,25 78:25,25 79:6 79:9,10,19 80:5,8,9,9 81:8 81:9,9,10,12,15 82:23,25 83:1,6 84:3,12 85:19,20,21 86:15,19 87:8,15,23 88:5 91:6,7,11,13 92:24 93:15 93:16 96:22 97:6,6,11,12 97:12,13,14,16,18,23,25 98:9,9,9,16,16 99:2,3,5,12 99:13,13,14,16 100:3 101:12,12,15,16 102:2,3	105:8,17,21,21,22,22 106:3,17,24 107:19,21,25 108:1,2,18,21,24 109:11 109:13 110:23,25 111:11 111:18,21 114:12,15,18 115:7,10,15,16 116:1,3 117:10,11,12,13,14,17,22 117:23,24 118:1,3,5,5,6,7 118:12,18,18 120:2 121:3 121:7,10,20,21 124:13,21 124:22,23,25 125:1,4,7,7,9 125:11,12,13,14 126:2,3 127:8,10,11,13,14,14,15 127:16 128:7,8,9,10,10,11 128:15 129:4,7,8 130:3,6,8 130:11,13,13,15,16,19,21 132:21,22,23,25 133:1,2,4 133:5,7,8,18,21,22,23,24 134:6,9,9,13,14,16 135:5 135:10,11,15,16 136:4,8 136:11,15,17,18,21,23,24 137:14,16,17,22,24 139:7 139:8,13,22,24 140:3,4,6,7 140:7,9,11,12 141:11,14 141:21,23 142:9,11,12,15 142:15,16,17,20,22 143:9 143:12,13,14,15 144:1,11 144:12,13,14,17,22,23 145:1 146:7 147:10,12,12 147:13,14,14,17 148:20,22 149:1,2,17,19,20,20,21,22 149:23,24,25 150:1,8,9,13 150:20,22,23 151:2,3,6,8,9 151:25 152:15,17,19,20,21 152:21,22 153:2,4,21,22 153:24,25 154:1,2,20 155:14,16,18 156:3,3,4,4,7 156:12,16,17,19 157:4,7,8 157:9,9,12,13 158:6,9,9,16 158:17,19,20,23,24,25 162:10,11,12,13,14,16,17 162:19,22,23 164:1,2,7,22 164:23,25 165:3,12,13,19 165:19 168:11,13,15,15,18 169:6,8,9,10,14,17,19,20 170:5,6,8,9,11,13 172:3,7 172:7,8,21,22 173:4,5,5,6 173:7,11,11,12,14,16,21 173:22,22 174:6,9,13,14 174:16,17,19,19,20,21,22 175:5,8,11,12,13,14 177:13,13,19,20,21,21,22 177:25,25 178:13,14,16,17 178:18 179:1,2,18,19,22 179:22 180:1,9,11,12,15
---	--	---	---

<p>181:9,11,15,16,21,23 183:9,23 184:4 185:21,22 185:22,23,24,24,25 186:1 186:2,4,10,11,13,21,25 187:1 188:4,5,6,8,8 189:25 189:25 190:1,2,4,5,8,11 191:13,14 192:3,4,5,10,10 192:11,13,13,14,15,16,20 192:21 193:12,12,13 194:17,17,18,19,20,21,25 195:1,2,5,6,17,18,19,20,23 196:2,13,14,17,19,20,21 196:25 198:8,9,13,15 200:15,16,16,18,20,21,21 200:22,25 201:1,3,22 202:2,4,6,6,14,15,15,16,18 202:23 203:14,16,18,19,19 203:21,21,22,23,24,24 204:1,12,16,17,18,19 205:2,19,25 206:10,11,12 206:14,15,17,17,17,19,22 206:23 207:2,2,4,4,8,15,16 207:18,20,22 208:20,20 209:2,4,5,9,22,24,24,25,25 210:5,6,10 211:14,14,16 211:16,17,18,20,25 212:1 212:2,2,4,9,9,12,12,14,14 212:17,21,21,22,24 214:7 214:7,15,16,16,17,18,22 214:24,25 215:12,13,15,18 215:21,21,22,23,24 216:2 216:3,4,6,9,10,16 217:5,11 218:17,19,20,20,21,23 219:12,21,22,23,24,24 220:2,2,9,9 221:13 222:14 222:23,23,24 223:5,8,9,11 223:11,21,22,23,25,25 224:2,11,12,12,15,16,18 225:6,6,7,9,11,11,18 226:15,17,18,23,25 227:7 227:20 228:20,23,25,25 229:1,3,3,4,5,6,7,10,10,12 229:13,13,17,20,22,23 230:1,1,2,4,5,6,16,17,18 230:18,19,20,22 231:14 234:1,2,3,3,4,5,6,7,8,11,11 234:13,15,16,16,20,22 235:5,6,6,7,9,10,14,15 236:2,4,6,8 237:21,21 238:4,5,6,7,7,17,17,18,22 238:23,24,25 239:2,20,20 239:21,25 240:12,12,15,19 240:20 242:6,6,7,8,15,16 242:16,19,22,25 243:9,14 243:24 244:3,6,7,7,8,10,16</p>	<p>244:20,21 245:15,17,18,20 245:22,22,23,24 246:2,9 246:10,10,11,13,17,17,17 246:19,21,22,24 247:13,15 247:17,18,23,25 248:3,5 248:20,20,21,22,22,23,24 248:25 249:1,2,3,7,11,13 249:14,15,16,18,23,25 250:1,6,7,8,8,9,12,15,17 250:25 251:17,20,21,21 252:3,18,19,21,22,25 253:8,9,10,11,12,14,16,18 253:20,22,22 254:12 255:4 255:6,9,21,21,22 256:10 256:10,11,12,16,17,17,18 256:19,19,23,24 257:5,6,7 257:8,12,16,16,17 258:2,5 258:6,6,7,9,10,11,13,16 259:10,12,12,14,17,18,21 259:22,25 260:1,3,4,6 261:13,14,15,16,17,19,20 261:21,22 262:21,23,24,25 262:25 263:2,3,4,6,16,22 263:23,24,25 264:3,3,10 265:16,16 266:4,5 267:3,8 267:9,11,18,25 268:4,7,11 268:21,21,22,23,23 269:2 269:3,5,7,7,8,12,12,13,14 269:15 271:18,19 272:13 272:14,16,17,17,18 273:1 273:2,3,23 274:4,5,23 275:1,1,3,5,5,6,11 276:18 276:18 277:10,17,18,18,19 277:20,21,21,23,24,25 278:1,3,8,8,10,18,24,25,25 279:2,7,10,10 280:1,2,3,4 280:7,7,8,8,9,25 281:1,1,2 281:4,5,6,8,9,11,12,13,22 281:23,23,24,25 282:4,7,7 282:8,12 283:10,10,11,13 283:14,16 284:3,4,20,21 284:23,23,24,24 285:1 286:16 287:18 288:1,2,3,4 288:4,6,8 289:22,24 290:1 290:21,23 291:2,2,16,17 293:4,6,16,18,20,20,21,21 293:25,25 294:1,2,3,5,6,6 294:7,8,19,20,20,21,22,24 295:1,1,8,8,9,13,23,24,24 295:25 296:2,2,5 297:4,6,6 297:8,8,11,13,14,14 298:11,11,12,13,17,18,19 298:20,21,22,24 299:1,7 299:12,12,15 300:1,1,3,5,6 300:7,7,7,18 301:15,15,16</p>	<p>301:17,22 302:11,19 304:15,16,17,17,21,23,23 304:24 305:10,24,25 306:3 306:4,5,8,9,14,15,16,17,20 307:9,10,12,13,15,15 308:21,23,24,25 309:22 310:9,9,10,11,11,14,18,19 310:20,21,24,25 311:12,12 311:15 knowing 262:20 knowledge 35:2 49:2 51:11 knowledgeable 67:6 known 51:18,21 KRISTEN 3:8</p> <hr/> <p style="text-align: center;">L</p> <hr/> <p>L 4:12,17 labeled 132:4 labels 12:25 lack 213:23 279:16 laid 257:8 language 25:7,7 26:6 27:9 64:10,14 68:22 109:13 113:21 114:8 117:17,18 170:6 192:20,21 195:23 196:3 223:23 291:23 lapse 272:12 278:3,10 lapses 255:18,22,25 256:6 257:2 265:7 large 21:5 29:6 33:22 38:17 62:16 124:25 125:8,10 130:16 198:10 209:14 214:18 257:12,13 largely 263:18 larger 126:15 largest 90:5 laterally 273:7,19 Latham 2:19 3:16 4:4 11:17 11:19,22 12:3 44:25,25 45:2 49:9 59:17 60:3 61:4 61:5 124:17 138:21 204:17 launch 79:5,13,14,17 law 11:17 14:7 44:25 90:20 lawyer 52:3,9 57:1 68:23 layer 173:15 275:1 layered 119:18 275:6 layers 278:1 279:9 layperson 121:14 249:7 laypersons 121:19 lays 114:14 lead 244:6 271:14 272:13,17 272:18 273:4 Leader 6:11 92:13 leaders 112:8 141:14 202:20 229:3 300:9</p>	<p>leadership 106:22,25 107:1 111:20,24 134:8 leading 90:15,19 304:12 leads 272:6 leak 275:14 278:7 280:14,22 leaked 262:4 275:23,25 leaks 260:16 led 29:4 105:16,23 126:12 ledger 269:14 Lee 45:9,21 60:15 Lee's 45:10 left 88:2 181:5 185:2 262:1,6 303:18 legal 9:9 51:16 52:3,10,20 54:5 58:6 legally 80:16 81:3 length 310:12 lengths 246:18 let's 17:17 44:12 54:18,19 55:12,17 56:18 57:16 58:21 86:23 96:24 114:21 121:13 125:5 152:12 164:12 199:11 236:12 254:3 260:15 268:18,25 288:17 300:18 303:17 308:7 level 20:3,8,17 30:10,13 31:8 32:4 34:22 80:11 89:15 126:1 128:15 130:25 139:21 140:1 143:16 144:22 148:19 149:13 150:22 153:2,7 155:13 156:6,8 178:5,18,18 179:17,25 212:7 244:14 246:1 272:5 304:21 levels 112:1,5 134:13 liberty 34:9 88:5 91:20 110:3 License 2:10,11,13,14 life 304:5 lifecycle 33:3 198:1 203:16 292:12 293:1,12 294:12 303:20 304:16,22 305:2,7 305:10 light 238:8 limit 275:12 limitation 121:16 limitations 48:21 limited 87:7 93:20 105:14 line 52:15 148:1 315:4 lines 148:12 link 56:11 117:25 209:8 linkage 216:9 linked 161:13 211:3,8,9,11 212:3,15</p>
---	--	---	--

links 118:16 208:16 210:13 210:17,21 211:3,15 212:17 241:19,22 Lipner 294:11 list 62:7 64:16 listed 39:17 62:10 67:25 124:8 136:13,18 137:10 146:24 162:8 210:4 255:7 lists 133:6 250:6,7 literally 128:7 litigation 22:22 23:1 243:3 little 20:7 23:9 27:19,22 49:3 73:7,17 74:7,11 75:5 97:1 125:21 126:21 129:1 147:23 183:7 196:5 197:24 214:1 247:2 271:8 303:18 live 211:3 LLC 77:16 LLP 3:16 4:4 location 133:20 297:23 locations 126:11 174:17 Lockheed 93:3 logging 46:25 47:1 65:18 173:7 login 218:9 220:4 221:3 273:6 logins 221:11 long 61:21 92:10 100:18 101:6 173:5 182:8 longer 58:22 89:2 92:19 look 35:12 40:22 42:19 47:3 47:8 48:1,3,4 57:4 58:13 62:25 69:16 82:3 83:14 85:23 92:11 95:13 104:11 112:13 115:7 116:6 120:6 122:13,17 125:6,9,10 128:18 131:10,16 134:24 136:6,24 137:8,19 140:16 142:6,21 144:8,23 147:9 147:17,19,21,25 149:3,10 149:11 150:2 153:1 155:24 156:25 158:23 160:21,21 164:12,22 166:10 169:12 172:12,19 175:19 176:8,9 178:21,21 179:25 182:21 186:17 187:5 188:5,12 192:23 196:18 200:6,17 209:12,16 210:8 211:8,10 211:11 212:2 215:3,9 216:20,21 218:3,7 220:13 234:12 236:12 238:7 239:21 240:13,14 241:1 242:6,10,15,25 244:1 245:11 250:5,19,25 254:12 257:5 258:11 263:15	264:11 266:3 268:22 271:19 275:3 276:19 282:15,24 286:9,19 294:17 297:19 looked 38:12 60:11 63:18 94:15 104:20 118:3 119:25 124:23 126:8,9 128:13,17 128:20 129:11 130:17,21 132:22 138:2 139:18 141:19 153:23 159:11 162:6,11,16 163:2,24 167:23 168:3,23 169:13 171:17 172:1,4,15 185:22 204:11 205:1,2,23 209:14 211:15 214:1,16,16 215:6 236:3 244:4 246:9 264:24 282:13 306:23 310:18 looking 24:16 37:10 38:6 64:8,11,14 65:5 69:3,4,8 70:8,12 71:6,16 77:23,25 78:1 112:7,8,11 113:17 120:7 121:25 138:25 142:16,17 143:7 144:19 146:6,8 147:24 148:4,14 148:20 150:5 155:16,20 164:24 165:25 172:17 173:10 175:4 176:19 179:16 193:2 197:8,12 209:20,23 212:5 228:11 230:7 235:10,22 243:6,18 243:19 251:21 256:20,22 267:21 275:4,5 279:5 282:22,23 287:12 295:2 297:14 306:1,18 looks 67:7 82:3 118:2 155:12 174:5 201:24 209:8 LORY 3:9 loss 30:7 lost 264:3 lot 15:19 26:3 35:4 36:18,19 41:18 117:25 118:16,16 134:9,11 157:5 158:18 164:3 165:22 177:15 178:4 178:6 181:12 210:6 218:21 223:19 228:24 229:12 246:9 247:14,17 252:21 262:22 268:5 282:14 296:6 297:7 lots 75:25 130:8 203:25,25 low 93:15 208:20 209:4 224:17 lunch 122:4 138:11 M M 4:5 286:9,20	magnitude 258:9,12,16 261:15,20 277:21 281:3 MailAssure 6:23 main 42:22 maintains 289:2 290:23 major 16:18 258:23 259:7 281:8 making 25:11 52:23 98:22 99:7 115:25 150:25 223:21 240:17 265:14 Makins 147:14 148:18 Man 49:18 manage 93:16 113:6 114:4 186:25 managed 93:11 127:17 management 82:22 89:15 137:25 142:18 144:17 148:24 150:16 170:11 190:1 195:1 196:6,8,11,13 197:7,11 213:19 manager 176:14,18 177:10 178:3,11 managers 71:8 managing 86:1 manner 187:11,23 map 134:18 162:12 212:4 mapped 207:16 mapping 139:15 150:23 maps 135:12 Mark 147:22 148:1,13,17 marked 6:4 7:4 8:4 41:23 42:1,15 43:13 91:22 92:1 99:18,22 119:1,5 131:6,11 147:1 159:5,9 171:11 176:23 199:21,25 205:6,10 217:2,15 231:24 232:7 237:9,13 240:22 285:9 market 83:1 Martin 93:3 Maryland 2:19 master's 13:17 45:15 match 27:5 57:15 135:1 matched 26:9,20 material 41:5 72:7,18 211:17 217:5 264:19 materiality 103:1,3 materials 62:7,10,13,14,16 matter 9:14 67:25 68:6 130:5 258:1 276:16 mattered 280:21 matters 89:6 Matthew 3:18 91:6,7,8,9,17 93:25 maturity 38:8 112:1,5 Maurice 4:6 161:1	mean 21:10 36:18,24 38:18 49:19 59:5,10 68:21 73:10 74:2,3,9 75:18 80:3,16 84:17 86:15 88:4 91:1 95:23 97:23 99:3 100:23 106:8 108:16 109:7 110:10 114:17 115:23,25 116:19 116:20 128:7 129:4 133:22 135:8 137:14 140:2 141:6 141:11 145:24 147:16 149:11 150:25 151:12,16 153:4 155:9,22 156:11,21 158:17 170:16 172:6,25 176:22 188:2 192:8 193:10 196:11 221:7 222:23 223:7 225:18 228:22 237:20 239:19 240:10 247:7,16 251:12 252:2 254:4,6 257:11 259:17 261:8,9,13 261:17 266:12,13 269:9 272:11,23 274:4 277:15 281:11 283:24 284:19 286:13 287:17 289:21 297:7 298:9 299:15 300:2 301:13 304:8 309:22 310:4 310:7,7 311:14 meaning 72:7,18 114:25 117:1 189:14 232:15 233:21 247:11 means 54:7 121:24 193:11 194:10,21 259:13 295:24 304:18 meant 101:14 115:13 121:7 121:20 134:9 180:14 190:4 196:24 201:24 202:7 232:23 233:15 240:19 247:19 251:10 252:17 279:10 measures 68:9,11,24,25 191:9 192:12 194:11,22 measuring 269:16 mechanism 306:5 mechanisms 141:17 medium 208:20 209:3 meet 61:5,8,21,24 113:3 114:1,18 303:13 meeting 151:9 MELTON 4:15 memo 58:22 92:21,23,24 93:5 memory 254:18 mention 40:4 277:14 mentioned 16:24 17:19 18:11 51:5 79:12 98:13 120:4 126:17,21 132:17
---	---	--	---

180:24 196:5 207:23 228:17,23 277:11 279:12 295:8 309:19 mentions 79:23 96:19 148:1 mere 126:24 Merit 2:6 message 184:14 messages 184:10 185:19 met 10:5 120:15 139:15 212:21,22 methodology 70:18,20,24 126:7 213:7 metrics 29:13,23 269:9,17 Michael 294:10 Microsoft 34:8 186:3 293:20 293:23 294:11 296:10 303:24 304:9 Microsoft's 216:4 middle 58:12 73:6 198:18 252:7 military 13:10 28:1 261:24 million 83:12 87:20,21,24 88:3,9,10 90:10 94:20 267:23 mind 151:11 200:3 221:2 232:14 233:20,25 234:24 245:9 291:4 mine 14:11 minor 43:7 44:7 224:11 226:16 minute 154:9 295:14,15 minutes 50:19 122:3,7 131:4 135:21 273:8,21 302:22 misapplication 263:2 misbehavior 262:23 mischaracterization 90:13 143:22 168:8 184:19 mischaracterizes 184:21 misconfiguration 273:1 misleading 53:24 54:8 55:21 56:11 57:3,8 72:23 153:10,15,17 misrepresentation 58:15,18 59:15 misrepresented 58:10 missing 130:17 160:9,11,17 160:23 192:21 230:11 misstatement 55:2 mistake 104:20 258:22 259:6 261:3,17 mistakes 261:19 mitigate 271:16 272:7 mitigation 236:9 248:9,15 model 36:6	modeling 34:14 35:5,7,10 35:19 36:9,15,22 37:9 39:11,19 207:8,10 231:11 232:14,16,21,24 233:11,20 233:22 234:4,7,9,13,17,20 234:24 235:2,4,8,11,12,17 236:1,7,18 238:12 239:3 240:1,21 242:17,19 244:9 244:12,17 246:7,8,12,13 246:22 247:4,12,13,20,21 248:2,9,13,17,22 249:9,12 249:19,21,24 250:4,10,14 252:11,19,22 253:5,7,14 253:23 295:5,7,12,20 296:2,7,11 305:8,11 modify 27:4 modifying 27:9 moment 44:13 50:14 118:3 154:21 183:14 191:12 200:4 217:5 Monday 61:14 monitor 19:3 monitoring 19:1 20:14,16 20:22 month 50:12 months 275:15,24,24 morning 10:3,4 motion 48:25 Motors 112:21 114:22 119:25 move 81:22 83:7 134:12 231:16 273:7,19 moved 169:17 202:16 movement 215:18 moves 260:22 moving 87:24 94:24 198:11 MSP 7:15 165:10 232:23 233:12 235:21 236:1 multiple 157:8 186:11 235:15 multiyear 256:1,7 mute 110:13 mystery 49:18	narrative 194:19 narrow 190:2 nascent 14:21 nation 17:5 national 34:22 35:22 92:18 112:25 115:19 116:22 native 8:5 171:22 285:13 natural 38:18 nature 106:22 137:20 147:16 256:12 298:23 necessarily 36:15 87:15 189:20 195:24 222:22 225:17 226:23 249:11,19 250:10 275:11 287:25 311:13 necessary 20:22 24:21 137:20 143:5,9,16 144:8 144:25 149:3,9 150:22,24 167:21 168:6 174:3 175:3 212:7 287:22 308:25 need 10:22 20:20 27:23 28:10 30:23 39:13 53:6 80:14 102:4,5 117:9 121:3 121:10 131:10 134:24 138:4 142:5 143:8,11 154:22 166:6,7 167:7 170:14 179:22 183:11 192:3,17 195:2,3,6 210:8 229:17,25 231:12,16 241:23 268:14,14 274:22 288:8 291:24 need-to-know 168:12,17 169:24 175:7 need-to-know/least 143:5 167:20 168:5 175:3 needed 103:16,20 149:17 150:4 178:1 212:22 218:14 260:17 287:16,22 288:10 needs 34:17 53:5 192:12 218:11 222:11 225:22,25 238:24 293:5 negative 279:1 neither 260:13 network 15:10,18 18:25 20:14,16,22 31:5 273:8,20 288:16,21 290:20,21,23,24 292:1,4 297:15 298:16 299:23 302:17 network-based 298:13 networks 19:2 28:24 never 38:9 59:23 240:14 242:15 274:23 new 1:2,17,17 2:9,15,16,18 2:20,20 3:20,20 9:4,4,13 9:13 44:17 132:24 133:20	133:21 269:1 313:23,23,24 newly 124:1 news 51:13 88:7,11 92:22 nice 303:13 nine 146:24 149:6 NIST 35:21 99:16 104:8,17 105:1,11,18 106:1,7,13,14 107:20,23,25 108:3,9,13 109:9,13,23 110:7,21 111:3,14 112:1 113:2,5,22 114:3,14,17 115:5,9 116:3 116:7,17,22 117:4,10,18 117:24 118:2,23 119:17 120:11,18 121:6 non-litigation 243:21 noncompliant 270:1,14 nondisclosure 25:14 nontechnical 18:7 normal 173:1 301:20 North 4:7 Notary 2:17 313:24 notation 215:20 233:8 286:21 notations 213:22 215:14 note 118:21 142:2 147:21 165:4,9 noted 9:16 210:24 312:4 notes 147:20 179:1 notifying 298:18 noting 194:25 234:8 notion 37:4 121:4 162:17 224:8 289:22 297:4,13 November 6:6,8 7:13 44:4 62:19,20 66:7 nuance 301:18 nuclear 260:17 number 22:2,2 29:6 38:16 42:4,4,5,11 77:2 87:8,9 88:6 108:18 124:23 125:10 130:16 131:15 139:13 171:16,23 172:10 177:2 190:16 197:14 200:2 209:14 231:2 255:25 256:6 257:2 266:13 267:11,13,22 268:25 270:3,14,15 numbered 93:15 172:9 numbers 25:18 33:22 90:10 160:22 161:23,25 231:3 257:12,13 numerator 265:23 266:10 266:14,20,25 267:1 268:1 268:3,7 269:25 270:13 numerators 269:18 numeric 188:23 numerical 257:11
--	---	---	---

<p>numerous 26:11 33:13 66:25 111:13 155:4 159:12 263:2 277:15 281:1 NYACR 1:23 NYRCR 1:23</p> <hr/> <p style="text-align: center;">O</p> <hr/> <p>O 4:12,17 O'Shea 218:8 o0o-- 4:23 8:11 oath 9:22 11:4 150:17 314:12 object 16:11 17:23 18:14 19:7,18 20:5 30:2 31:17 32:12 40:10 41:7 44:21 46:10 52:7 55:3,23 56:23 56:23 57:24 63:2,4,20 64:18 70:9 72:9,25 73:21 74:25 76:6 80:2 88:23 90:25 102:1,19,24 103:4 107:16 108:15 111:5 116:12 128:4 130:2 132:3 143:21 157:3 158:5 168:7 169:2 180:6 189:17 208:24 210:23 214:4 215:11 219:7 226:11 240:9 243:8,23 247:5 254:9 255:2 258:25 259:9 261:6 272:10 275:19 287:24 288:15 292:14 296:20 311:7 objecting 185:12 objection 47:17 89:1 98:6 98:25 99:10 103:13 109:25 127:3,4,6,25 133:12,17 134:5 137:12 165:18 181:7 184:12,16,18,18,25 189:10 193:18,25 194:1,15 195:11 202:13 218:15 222:21 225:4 248:19 271:17 273:9 274:12,14 279:19 280:16 291:9 299:20 304:12 308:20 objections 103:20 obligated 110:25 291:16 obligation 87:11 195:20 obligations 87:10 observed 140:10 obviously 10:13 11:3 160:8 218:4 262:16 occur 219:23 263:23 265:7 occurred 19:4 54:1 135:18 246:19 259:22 264:5 occurrence 267:9 occurring 244:17 252:22 253:15 283:17 298:19</p>	<p>occurs 102:21 123:6 163:18 227:20 231:21 267:6 270:5 273:11 290:16 307:23 308:14 October 50:11 54:1,19 55:18,19,20 57:18 62:19 62:20 67:15 200:14 offer 21:16 47:15 48:21 52:10 314:11 offered 103:2 offering 47:11 54:1 69:8 153:7 offers 22:6 officer 81:24 82:24 83:9,16 85:11,25 86:9,18 89:13,14 89:16,20 91:10 92:20 93:8 93:25 94:17 96:5,9,10,16 107:2 oh 42:24 53:14 109:14 122:16 132:5 146:7 148:8 154:11 166:21 178:13 190:21 208:8 228:13 okay 10:19 11:7,9,18 12:2 12:13,23 13:2,5 14:12 15:17 16:3,6 17:17 18:11 18:18 19:15 20:19 21:7 22:6 24:8 25:8,22 26:18 27:18 30:16 32:10 34:13 39:7 41:8,14 42:12 43:2,11 43:20 44:11,19 45:10,24 46:13 47:5,10,25 48:17 50:2,9 51:4,20,23 52:19 55:16 56:15 57:14,23 59:16 60:9 61:5,12,17 62:24 64:7 65:8,11,25 66:8 66:23 69:2 70:22 71:1,4 72:21 73:3 76:17 78:2,6 79:12,23 80:13 81:4 82:11 83:7,7 84:7,15 85:8,23 86:23 88:1,18 90:8 91:6,11 92:11 93:1 94:6,13 95:12 95:24 96:3,24 98:2,12 101:22 102:7 103:7,20 104:24 105:1 106:6,25 107:12 109:6,7 111:1 112:13 114:21 115:17 117:3,20 120:6 124:19 126:12 132:5 133:11 134:24 136:11 137:6 138:22 139:10,17 140:15 140:22 141:8,24 142:25 144:7 146:13,17 147:19 148:11 149:13 153:13 154:20,24 155:1,2 156:10 156:23 157:17 159:4,17</p>	<p>160:18 161:16 162:3,24 163:13,23 164:10 165:7 166:24 167:2 168:10 170:22,25 171:20 172:17 173:18 175:16,25 176:7 177:4,7 178:9 179:11 180:2,23 182:22 183:13 184:7,15 185:4 186:6,15 187:18,20 190:17 191:17 191:18 192:23 194:3 195:10 197:5 198:16 199:11,12 200:9 202:1 203:2,4,7,8 204:5 205:9 210:11 211:7 213:9,15 214:11 215:6 216:13 217:1 217:8 218:2 219:3 220:4 220:18 221:24 222:3 223:13 226:6,22 227:16,23 227:25 228:13 230:10,25 231:9 232:2 236:12 239:4 239:9 240:4 241:7 242:21 244:24 245:8 246:5 248:8 249:6 251:3 254:8,19 262:14 264:22,24 265:1,18 268:18 269:12 270:19,22 271:13 272:3 273:5,16,16 278:5 279:12 280:13 282:19 283:1 284:10 286:8 286:19 290:4,10 291:13 294:15 295:4,11 296:9,13 296:22 297:19 299:3 300:20 302:21 309:18 310:2 once 52:19 54:5,15 164:10 181:11 193:16 199:5 261:1 262:4,10 273:5 one's 190:9 309:1 one-year 176:12 179:13 ones 19:22 119:24 ongoing 174:8 230:18,20 open 77:12 operating 91:10 178:19 291:17 operation 20:25 67:8 operational 28:8 operations 16:15,20 82:1 93:25 opinion 26:14 39:25 52:10 54:6 68:24 70:10 103:2 115:4 153:7,11,13,20,22 158:2 166:14 216:8 254:23 255:15,18,25 256:6,18 257:3 265:9 276:10,11 opinions 47:10,15 48:22 52:3 66:12 104:8 214:14</p>	<p>251:6 opponent 48:25 opportunity 83:1 246:6 opposed 134:3 opposite 129:24 options 82:15 orange 291:4 order 32:6 37:10 38:20 67:6 121:21 131:15 150:9 151:4 163:9 173:2 192:13 218:5 294:6 304:19 309:2 ordinarily 67:2 ordinary 166:11 organization 24:11 26:9 28:23 36:3 37:15 38:17 39:1 198:10 248:25 258:24 259:18 283:7 293:16 295:18 organization's 36:9 259:8 organizational 34:22 119:16 organizations 16:19 28:9,12 28:13,19 29:4,7 30:22,24 34:21 35:9 36:4 39:15 40:18 41:21 76:12 196:19 294:2 296:1,4 organizations' 36:6 118:14 organized 174:5,13 210:2 orient 145:17 original 44:4,9 51:17 100:6 263:8 originally 96:8 163:16 origins 196:23 Ortega 4:19 9:8 outcome 249:19 313:11 outline 231:3 outlined 115:7 136:21 173:16 206:20 207:12,15 229:24 246:16 289:5 307:14 308:5 310:10 Outlook 133:5 output 174:20 249:8,22 250:2,5 outputs 79:9 111:21 173:6 204:19 249:23 250:4,11 outside 67:3 71:16 98:7 103:5,9,11 130:10 137:3 138:2 141:18 142:21 150:18 151:16 157:7 183:24 184:2 186:7,18 243:3 overall 17:13 195:19 229:2 244:16 overarching 76:2,14 overlapping 247:25 overlay 161:12</p>
--	--	--	--

overlaying 163:11
oversaw 83:11 94:19
oversee 87:3,6,21 93:10
overseeing 197:25
overseen 32:14 66:25
oversight 17:25 18:10 28:16
 32:23 34:3 79:1 81:9
owner 82:11
owners 101:20

P

P 3:1,1 4:1,1,12,17
p.m 2:23 138:9,12,12,14
 182:12,15,17 228:2,5,7
 270:24 271:2,4 303:2,5,7
 311:21 312:4
page 5:4,10 6:4 7:4 8:4
 42:20,22,23 53:14,15
 66:23 73:4 78:1 83:15
 85:24 92:12 93:1 95:14
 96:15 100:9 104:21,22,25
 109:17,18 112:14,15,17,20
 118:1 119:16 120:6 122:13
 122:17,24 131:16 140:19
 140:20 145:5,11,19 146:4
 146:9,10 147:10,20 148:6
 154:6,19 164:13 166:5,21
 170:21,24 171:1 175:17
 182:21 187:6,7 188:16,17
 190:15,18 193:2 197:14,15
 198:17 201:5,11,12 203:2
 208:4,5,9,9,11,12 213:4
 216:14 217:23 220:18
 221:19 231:2,8 236:15
 237:25 250:21 264:12,13
 277:7 282:18,25 285:23,24
 285:25 286:7,9 297:22,22
 297:25 301:2 315:4
pages 5:9 122:24 123:17
 198:17 208:7,21 285:22
paid 12:2,5,11
painful 260:10
paragraph 53:11,12,15
 66:24 69:24 73:4,6 77:15
 78:7,13 81:23 83:8 84:8
 92:15 93:21 94:14 100:11
 104:12,21,25 109:19
 112:16 113:11 114:25
 122:18,19 123:2,10,14,19
 143:2 145:5,9,10 154:6,19
 154:21 155:3 158:8 159:11
 162:18 166:23 167:5,11,22
 170:20,23,24 171:3,6,14
 173:12 175:18,19 176:10
 177:8 179:6 180:14,23

181:11,16 182:21 183:16
 186:3 187:6,9 190:15,22
 190:24 191:14,19 193:4
 194:6,13,18 195:4 196:1
 197:17 198:17,18 199:6
 203:2,5,8 204:5 210:11
 213:2,16 216:14 223:14
 231:1,3,6,7 232:2,10,12
 233:7 236:15 237:15 238:9
 238:10 240:11 241:2
 244:24 245:15 249:14
 250:19 252:7 264:12,19,25
 265:1 277:3,9 282:16
 288:24 297:20,25 298:2
 300:13,18,19,19,24 302:2
paragraphs 216:17 223:16
parameters 206:1
parentheses 113:2 210:14
 237:4
parenthesis 213:21
part 29:9 33:24 40:21 48:18
 80:7 84:7 86:24 103:9
 127:10 134:22 141:6
 143:11,14 144:1 145:15
 179:5 184:24 201:3,21,23
 201:23 202:18 207:9
 232:22,25 233:11 234:9
 239:25 241:1 246:14
 248:17 250:14 282:1,22
 292:11,25 295:1 307:19
participant 110:11
participation 80:10
particular 39:21 41:4 55:5
 76:18 114:2,19 120:15
 150:3 153:24 172:1,9
 178:15 181:19 183:1
 198:24 215:4,9 223:17
 228:18 239:16 240:6
 270:16 278:13 281:2,4
 306:8 307:17
particularly 31:21 35:13
 62:16 64:5 309:1
parties 102:21 119:7 123:6
 163:18 231:21 267:6 270:5
 290:16 307:23 308:14
 313:13
partner 77:16 95:17,22,25
partnership 86:17,22
partnerships 83:10,17,24
 84:6 85:12,25 86:10 87:6
 88:21 89:5,10,12 93:18
 94:18 96:17 105:24
parts 190:11
password 30:6 31:1,2 38:11
 57:17,21 58:4,23 74:5

182:24 185:24 186:4,14
 187:11,23 188:21,25 191:8
 192:11 193:6 194:11,22
 195:7,13,19 218:24 219:13
 219:18,22 220:11 226:10
 268:20,23 269:1 271:8,11
 271:14 272:5,14 274:10,22
 275:14,23 276:4 278:7
 280:14,21,23 281:12
 305:18 306:20
passwords 188:22 191:7,25
 194:9 196:4 216:7,11
 221:11,17 225:9 227:4,14
 260:16 268:18 270:1,14,15
 306:7
path 283:14
Paul 89:17,22
Pause 47:18 146:16 154:25
 171:10 176:6 183:12
 187:19 191:16 199:10
 200:8 203:6 205:22 213:14
 217:9 264:23 300:21
pays 12:3,7
PDF 209:9
Peak 45:18,19 77:16 78:8
 82:6 83:4 95:17 100:12
 101:16 243:14,22 311:4
Peak's 99:23
pen 81:17,19 212:24 297:18
 298:25 300:6 301:17,19
 311:8
penalty 5:13 314:4
pending 10:25
penetration 17:10,15 78:15
 78:21 79:3,6,15 210:18
 296:17 297:2,8,12,16
 298:4,12 299:4,10,15,18
 299:21,22 300:3,14 301:5
 301:10 302:5,16,17,18
 311:4
Pennsylvania 2:18
people 22:5 31:9 36:19 38:2
 39:23 65:4 67:5 79:19 81:8
 87:14,16,18 97:20 107:3
 108:18,19 110:13 111:19
 115:25 121:24 130:21
 144:12 190:1 219:25 221:8
 232:21 246:3 247:18
 262:20 291:2,7 292:2
 297:11,17
per- 284:2
perceived 213:6
percent 55:8,9 157:23,24
 254:24 257:23,24 269:12
percentage 157:1 269:9

295:25
perfect 255:6
perfection 156:22 190:10
 255:9 256:16,24 259:15
perfectly 156:19
perform 28:24 109:22
 243:22 299:10
performance 39:2 235:11
performed 56:2,3,4 232:22
 232:25 233:11
performing 36:21 158:25
 159:1 290:7
period 25:21 53:25 54:4,19
 54:22,25 55:8,9,22 56:5,13
 56:19 57:22 58:13,25 59:9
 59:12,14 60:12 62:12
 67:15 69:13,18 84:4 85:13
 85:22 88:10 107:18 118:4
 119:9 124:2 126:9,18
 134:14,14 145:14 153:8
 155:7 157:15 176:12,13,17
 177:9 178:1,10 179:7,7,13
 179:14 180:3,4 183:25
 184:2,6 186:7,18 198:8
 200:14 253:17 256:1,7
 305:14,19,23 306:17,21
 307:4,8,12,16 308:4
 309:15 310:4,6,14,16,21
 311:1
perjury 5:13 314:4
permissible 81:3 186:17
permissions 157:25 287:16
 287:19 288:5
permitted 272:1
person 34:20 61:13,16
 108:17 132:22 135:5 136:4
 136:10,16 149:15,16
 176:12,17 177:8 178:1,10
 313:8
person's 136:14,19 229:18
personal 260:9
personally 12:14 16:9 34:13
 39:10,17 40:8 51:7 60:10
 62:9 78:20 79:1,25 111:2
 111:25 262:21
personnel 83:12 86:25 87:3
 87:6 94:20
perspective 172:22 207:1
 263:7 294:8
pervasive 255:19,21 261:9
 261:22 265:17 266:2
pervasiveness 265:14,25
phase 206:24 207:22,22
phases 207:15
PhD 13:20 14:3,5,9,12,16

<p>15:3,5,9 16:3 phone 3:12,21 4:9 65:21,23 90:9 phrase 191:22 194:13 304:4 phrased 276:20,22 physically 80:5,6 pick 126:6 303:17 picking 156:23 piece 141:22 pinned 304:23 pivoted 289:24 place 16:21 19:2 38:8 66:5 67:4,14,20 68:9,12,19 69:3 70:15 71:24 73:16 125:18 127:12 130:7 136:25 138:1 138:3 140:5,11 141:20 144:21 148:24,24 151:4,12 152:20 162:19 170:15 174:24 186:10,21,24 187:2 190:7 192:17 196:21 212:25 213:20 253:17 269:18 306:21 310:21 313:5 places 172:25 186:11 198:3 209:5 210:16 266:1 277:16 282:12 305:12 plaintiff 1:5 3:3 68:6,15 plan 47:15 planned 88:8 plans 44:18 47:22 play 97:5,7 played 41:11 players 207:21 please 100:8 110:13 112:14 146:10 165:4,8 166:9 167:3 175:17 182:21 185:13 194:4 216:13 222:13 231:1 259:1 270:11 275:21 311:25 plenty 295:3 297:10 plural 123:23 point 10:22 19:9,12 44:3 93:16 111:12 136:19,22 147:23 177:14 181:11,18 186:9 201:1 216:5 221:25 223:20 238:11,11,14 239:1 239:23 240:11,18 241:22 244:5 245:15,16 277:1,1 291:6 293:19 310:18 poised 289:22 policies 29:10,12,15,22,24 37:16 69:3,5 70:14 71:9 214:17 219:24,25 policy 13:15,18 14:11 28:6 31:4 38:11,13 39:1 55:18</p>	<p>57:17,21 58:4,10,16,23,23 71:7 112:8 127:11 130:6 141:13 142:16 144:15 157:23 193:6 195:14,19 268:20,23 283:8,23 284:18 284:20 288:13 290:11,14 291:6,10 305:18 political 13:9 poor 271:14 272:5 portion 132:20 225:15 288:16,22 290:22 300:22 portray 101:15 pose 34:24 196:22 position 89:9 positions 95:19,21 96:6 possible 56:22 151:21 152:6 152:11 269:15 273:24 278:11 305:6 possibly 263:13 post 210:13,17,21 post-2015 69:16 posture 23:12 25:6 120:18 postures 26:12 potential 121:22 194:25 229:6 278:25 potentially 52:13 197:9 PowerPoint 73:13 215:16 practice 35:8 46:24 56:3 64:12 69:1 71:22,22,24 93:18 108:2 112:12 124:3 124:14 125:8,15 137:22 142:12 155:6,13,15 170:5 192:19 227:14,17,19,21,22 229:2,8 230:5,9,11,14,19 234:8 243:5 248:18 255:5 277:25 278:9 281:10,14 292:17 294:7 295:2,5,12 295:22 297:5 305:23 306:10,12 practices 27:1,5 28:15 52:24 54:21 58:7 64:6 70:1 70:2,5,7 71:15 73:8,15,18 73:25 74:3,8,12,18,23 75:6 75:10,24 76:1,5,20 97:22 98:4,15,24 101:24 102:14 117:6 121:23 140:5 144:13 157:10 184:8,11 185:17,20 186:16 188:22 190:7,11 191:6 194:8 195:7,23 196:3 197:1 200:12 202:12 215:1 229:23 234:12 254:25 256:11,17 257:18 280:23 292:9,22 294:20 295:9 297:3 304:24 306:20 307:7,13</p>	<p>precise 79:16 146:4 258:7 precludes 221:10 predated 310:3 predesigned 15:25 prefer 231:19 premise 103:25 104:4,6 preparation 61:6,18 prepare 60:23 61:22 preparing 62:8 66:12 presence 29:5 37:10 39:4 57:4 62:18 68:8 70:14 71:7 74:4 111:19 112:8,12 124:14 135:9 142:12 144:4 144:15 148:22 152:22 164:25 169:13 175:8 181:22 188:8 206:14 211:18 229:23 230:8 242:10 244:1 253:15 256:11 257:7,17 258:4 263:21 307:11 308:24 present 30:11 69:17 80:5,6 82:4 95:17,20 96:6,7 202:17 244:18 246:17,18 246:25 249:14 presentation 200:1,6 201:21 201:23,24 214:2,6,13 215:4,16,17,21,23 presentations 213:19 presented 133:25 181:21 201:25 202:4,7 President 92:18 260:23 264:7 pretty 19:20 32:8 41:16 54:11 87:11 125:20 133:19 151:6 162:21 169:4 174:16 195:17 200:22 202:6 206:17,18 225:7 229:14 233:1 259:24 282:13 296:3 303:16 prevalent 310:13 prevent 11:10 119:19 preventing 291:7 prevention 30:8 previous 245:14 previously 47:22 67:19 120:4 price 100:14 101:10 primarily 61:1 82:23 primary 186:24 253:13 principles 72:12 printed 171:21 211:2 prior 26:7 43:15 50:2 59:16 60:2 67:18 90:7 112:17 219:16 253:17 privacy 241:14 242:23</p>	<p>privilege 143:5,12,16 167:21 168:5 175:3 288:7 privileged 143:9 175:7 privileges 273:7,19 proactive 236:21 237:3,18 237:24 239:6 240:7 242:2 242:13 probably 24:24 25:20 29:1 31:11 57:8 59:14 61:10 66:7 69:11 79:18 81:13 83:5 87:16 90:12 92:9 97:24 108:19 110:2,24 117:11,16,23 130:20 137:15 146:7 165:13 170:3 172:25 231:6,22 250:24 269:7 276:19 280:10 296:6 297:10 problem 211:2 258:16 262:3 263:14 problematic 272:25 problems 213:6 279:5 procedural 28:7 180:1,13 procedure 31:4 71:8 127:12 142:16 180:1 185:9 188:9 procedures 28:21 29:11,13 29:15,19,23,24 32:24 37:23 71:10 274:21 294:21 298:16,19 proceed 63:22 167:3 171:8 199:11 205:24 proceeding 62:23 PROCEEDINGS 9:2 process 7:7 31:22 32:1 33:4 33:17,23 34:2,6,8 35:12,16 38:4 43:23 46:12,16 63:9 116:10 125:17,22 127:18 128:9 130:6,7,12 132:20 132:22 133:7,8 134:7,11 134:15,22 135:10,15 136:18 137:24,25 138:1,2 139:23 140:12 141:6 142:1 143:14 144:20 145:15,15 148:25 149:20,22 150:6,7 150:11,15,17 151:11,12,19 151:24 152:1,3,4,10,13,15 152:22,24 156:3 157:1 162:15,19 163:1 164:7,25 165:1,23 168:11 169:15 174:4,20,22 175:13 178:20 179:21,24 180:17 184:5 188:9 194:19 198:7,11,23 199:3,16 201:3 202:8,17 202:21 203:11,22 205:1 206:15 207:1,19 209:21 211:16 212:2,11,20 214:3</p>
--	---	--	---

<p>214:19,22 216:4 224:13 232:22,25 233:12 239:2,24 240:12,18 242:10,18 244:6 244:14 245:16 246:1,21,23 249:24 250:5 251:5 261:18 261:23 262:22 280:6 283:11,15,17 284:8,24 293:24 299:13 300:6 302:13 307:1,18 309:22 Process' 199:1 processes 16:16,17,22 25:4 32:5 34:4 35:3 37:2 40:21 126:5,22 140:5 151:3 156:5 173:16,25 202:22 204:4,19 206:20 235:8,13 249:13 258:4 263:25 308:24 309:2 310:11,22,24 311:1 produce 163:9 250:1 produced 160:4,13 161:4,8 161:8,11 162:2,10 163:5,6 163:10 211:4,10,15 249:22 294:11 producing 211:16 product 46:4 83:2 196:22 207:3,17,19 216:10 production 160:16 173:1,21 211:24 222:13,20 223:3 225:16 226:3 227:5 235:12 282:10 287:3 288:14 289:2 289:6,8,12,17,24 290:8,12 290:24 291:3,8,17 292:13 293:2,7,10 products 7:15 97:21 121:23 170:13 196:17 234:22 235:22 236:1 profess 72:21 professed 37:16 76:21 professes 76:5 professional 2:5 52:21 292:8 professors 14:20 15:20 proficient 79:21 program 14:5,10,13,16 15:5 15:9 16:3 17:3,11,21,22 18:1,8,10 28:17 29:10 34:12,16 38:4 39:13 83:11 84:9,11,16 85:1,4,13,17 94:19 106:24 108:5,22 112:25 115:18 116:22 174:24 265:7 programming 33:7 programs 16:14,21,22 17:9 17:13,14,16 32:14 263:21 prohibit 221:3 291:16</p>	<p>prohibition 220:11 project 35:16 promise 40:3 promised 250:15 promulgated 76:12 proper 124:23 137:4 143:15 157:11 196:20 properly 75:24 76:4 146:14 149:22 165:24 175:15 proposition 272:12 protect 68:20 188:24 protection 89:7 271:8,11 272:15 274:10,22 provably 59:7 provide 11:14 46:5,21 64:7 64:22 121:21 134:9 175:20 196:24 294:3 298:24 provided 29:14 109:12 212:13 provides 174:7 provision 103:18 143:13 150:10 165:24 provisioned 127:16 220:23 221:14 provisioning 132:19 143:15 175:14 221:8 provisions 28:18 30:7 225:7 225:8 public 2:17 13:18 23:11 24:2 25:11 27:13 45:17 53:25 58:24 72:5 88:7,11 97:7,25 98:14 99:7 102:9 313:24 public- 129:16 public-facing 23:17 24:10 24:14,19 26:6,19,21 27:10 97:2 220:6 publication 92:10 99:23 publicly 25:1 26:15 51:18 82:17 276:6 published 92:8 publishing 115:9 pull 287:18 purchasing 97:21 purport 208:16 purpose 97:19 114:11 170:16 180:7 190:2 274:5 purposes 12:16 97:25 216:19 252:14 pursue 53:4 pursuit 294:22,22 put 24:3 36:7,9,12 42:10 98:14 100:4 114:13 131:14 147:5 166:3 186:9 253:16 269:17 292:23 putting 23:13 107:12 111:1</p>	<p>125:3</p> <hr/> <p>Q</p> <p>qualifications 77:7 81:14 qualitative 257:20 quantification 257:15 quantify 267:22 question 10:17,25 11:1 16:12 23:14 24:15 30:17 31:13 32:18 52:2 54:13 58:9,11,11 70:4,17 71:2 72:15 74:20 76:18 94:2 102:5,5 103:22,24 108:7 110:17 111:12 116:11,15 121:2 129:2,9 135:3,22 137:6 139:3 143:1 151:13 156:13,16 169:4 172:23 177:7,24 187:17,21 191:2 194:4 200:10 205:25 209:1 218:22 233:1 242:25 243:10 245:14 251:23 253:2 259:2 267:10 269:23 271:21 273:25 274:15 275:18 277:10 279:24 286:17 291:21 309:10 questions 46:11 65:5 68:7 141:25 182:4 183:9 213:11 226:9 227:8 272:2 289:20 303:10 309:8 311:17 quick 74:15 95:13 154:20 172:19 205:17 217:5 258:10 274:21 278:20 300:20 quickens 279:9 quickly 10:12 60:22 140:15 229:14 271:15 272:7,14 275:10 276:12,15,17 278:7 278:17 279:4,5 280:14,22 297:19 quite 16:13 54:9 150:21 156:2 157:6 183:24 184:1 186:7 227:20 247:7 269:16 293:18 Quitugua 183:3,19 quotation 251:22 quote 109:11 112:21 113:13 120:8 167:13 237:2 quoted 101:16 252:25 254:15 quoting 109:14 118:22 146:1</p> <hr/> <p>R</p> <p>R 2:5 3:1 4:1,12,17 313:21 rack 38:25</p>	<p>RAF 285:15 range 97:8,9 rapidly 272:18 rare 38:24 Rarely 274:3 rate 60:6 158:21 265:4,11,19 265:23,23 266:8,11 268:2 268:10,20 269:12 rates 266:6 Rattray 1:15 2:4 5:2,11 6:2,5 6:8 7:2 8:2 9:15,21 10:3 42:14,15 51:4 91:25 92:16 93:4,10 95:12 99:21 103:2 119:4 163:5,15 182:20 205:9 228:10 254:22 271:7 303:9,17 313:3 314:3,16 315:2 RDR 1:23 re-rolled 133:7 reach 126:25 reached 126:20 129:24 read 23:2 53:12,19 79:8 113:8 121:15,16,19 143:8 145:20 146:14 154:21 160:5 162:20 164:19 165:3 165:8 166:7,25 167:5,6,7 171:6,13 176:1 187:15 189:6,15 190:2 191:3,13 191:19 192:14 199:13,14 203:4 205:16 213:10 217:5 220:10 226:17 237:18 257:12 264:16 289:12,17 291:25 294:10,14 300:20 300:22 314:4,6 reader 86:20 151:7 170:10 256:21 readers 145:2 255:10 reading 22:25 51:13,19 86:12,12 123:1 145:24 158:7 166:20 193:24 194:12 246:3 277:8 289:17 reading/reviewing 146:16 154:25 171:10 176:6 183:12 187:19 191:16 199:10 200:8 203:6 205:22 213:14 217:9 264:23 300:21 reads 85:10 ready 176:7 217:12 real 113:18 205:17 really 10:11 62:18 71:2 75:14,20 121:10 139:24 142:2 151:14 162:24 181:19 201:1 229:8 230:7 255:14 297:6 299:6</p>
---	---	---	--

Realtime 1:24 2:7,9,16 313:22,22,23 Realty 113:14,20 120:1 reason 94:2 117:7 128:11 141:24 181:12 186:22 210:3 246:15,20,23 315:5 315:6,8,9,11,12,14,15,17 315:18,20,21,23 reasonable 68:8,23 reasons 98:21 178:7 180:16 229:21 243:1 263:19 293:9 Reassigns 6:10 92:13 reassured 104:1 reassuring 100:19 101:6 recall 25:9 27:8,8 50:9 51:24 51:25 60:6 66:4 90:23 91:2 163:23 175:24 198:2 245:8 245:10 279:22 282:2 289:14 296:9 309:16,20 receive 44:17 received 15:3 62:15 63:9 79:10 123:25 124:17 145:13 149:16 155:4,11 159:13 163:15 204:7 receiving 29:23 recess 50:23 95:6 182:14 228:4 271:1 303:4 recipient 149:21,25 recognize 293:23 294:15 recollection 100:5 148:16 recommend 299:4 recommendations 117:6 record 9:7,17 10:18 42:18 50:22 51:2 95:5,10 118:21 131:22 138:10,15 154:16 160:25 163:4 176:25 180:11 182:13,18,24 199:24 205:11 208:6,22 228:3,8 232:8 237:12 241:10 260:8 270:9,25 271:5 285:12 303:3,8 311:22 313:7 RECORDED 1:14 2:3 red 16:15 17:10,15 78:16 79:3,23,25 80:15,24 81:5 81:16 130:19 298:4,13,25 redefine 132:23 refer 54:3,18 199:14 reference 146:9 183:17 200:1 217:18 260:9 referenced 192:19 referencing 160:8 referred 49:16 264:9 referring 225:15 226:3,16 226:19 288:23 299:2	refers 92:25 226:18 241:2 refine 24:21 reflect 48:9 165:10 280:22 reflected 66:20 118:23 reflecting 226:9,9 245:1 reflection 260:3,3 reframe 54:10 102:4 refreshes 148:16 regarding 113:22 167:14 175:6 184:10 185:19 191:18 216:11 236:1 248:6 regards 73:5 regions 126:19 Registered 2:5,6,7 313:21 regular 124:3 145:15 173:13 173:14 312:1 regularly 120:17 regulated 108:22 regulation 89:6 regulators 106:10 regulatory 106:11 107:4 rehear 102:5 relate 75:10 147:21 225:8 242:22 289:20 290:2 related 27:9,14 28:8 41:4 47:2,3 51:13 64:21 73:25 74:18,23 75:20 76:17 98:17 104:8 130:23 131:5 141:22 155:24 158:10 164:6 173:22 192:21 202:8 203:19,22 217:6 234:19 235:19,21 239:5 260:4 294:18 299:15 313:12 relates 30:1,17,19 31:15 147:11 148:17 relating 166:16 167:25 168:25 231:11 279:23 291:6 309:19 relations 14:4 relationship 11:24 relatively 19:23 20:8 releases 236:4 relevant 12:19 54:3 67:14 73:24 96:21 101:9 113:7 114:5 118:4 119:9 124:1 126:9,18 134:14 145:13 153:8 155:7 157:14 181:19 183:25 184:2,6 186:7,18 200:13 253:17 258:17 269:19 277:19 305:13,18 305:23 306:16,21 307:3,7 307:8,11,12,16 308:4 309:1,15 310:4,6,14,16,21 311:1 reliable 305:22	reliance 309:14 reliant 252:20 relied 184:21 185:21 214:2 252:16,21 310:2 relies 305:12 rely 150:13 184:2,9 185:18 200:11 214:13 229:19 243:5 relying 127:23 184:13,22 186:5 239:13 remark 180:8 233:16 remediate 278:10 remediated 276:12,15,17 277:12,19 278:7,25 279:3 280:14,21 remediating 278:17 remediation 274:9,21 278:20 remember 25:19 43:10 44:6 50:6 65:22 92:9 139:14,15 170:23 172:8 253:18 276:8 303:21,25 308:12 remind 15:2 52:1 remote 3:8,9,18 4:13 65:23 removed 88:16,23,25 render 256:1,7 257:3 reorienting 192:2 repeat 31:25 72:15 74:20 103:21 110:14,16 129:8 144:14 180:10 187:17 194:3 243:10 256:3 259:1 270:10 297:23 repeatedly 265:6 repetitive 115:16 116:2 120:5 replaced 93:4 report 6:5,7 35:20 40:3,4 42:22 43:6,8,12 44:4,10,20 44:22 45:3,6,25 46:6,25 47:9,12,23 60:5 61:1,2 62:8 66:21 73:5 77:3,9 79:11 84:1 85:9 86:12 88:12 89:12 94:14 96:18 103:3 104:13,14 109:12 112:14,20 117:12 118:23 124:18 127:7 139:1 149:8 153:23 175:17 177:8 181:15 194:2 205:5 208:19 209:6,9,13,15 210:4 217:18 223:13 231:2 232:3 232:5,10 236:3,15 250:19 251:7 252:4 254:15 255:4 259:22 277:4,16 278:22 282:16 285:17 297:20 300:12 305:12	reported 89:22 276:4,13 313:8 reporter 2:6,6,7,8,9,10,11 2:13,14,16,16 5:12 9:18 10:13 29:18 42:15 313:1 313:21,22,22,23,23 reporting 9:9 51:19 81:11 89:23 269:14 298:23 reports 29:5 41:18 46:22 61:3 88:8 127:14 175:4 208:2 209:15,16,23 210:2 210:2,7,9 212:1,5 299:14 repository 276:5 represent 12:6 59:9 64:20 117:3 119:6 146:23 159:10 representation 54:7 120:11 123:11 191:6 194:8 representations 53:24 122:21 151:9 166:15 167:24 168:24 187:12,24 188:11 representative 126:14 represented 56:12 57:5 58:24 representing 53:9 represents 86:6,8 reputation 49:22 request 65:6 124:13 132:10 139:24 140:13,14 142:2 143:24 149:21 164:16 169:16 requested 5:17 64:4 131:25 132:1 165:14 177:2 204:16 313:17,17 requesting 155:4 159:13 requests 64:23 102:22 123:7 139:8 141:18 270:6 307:24 require 14:13,16 15:5,9 16:3 69:15 115:11 220:23 required 28:14 80:16,17,19 80:20 274:6 requirement 107:10,12 requirements 31:16 52:20 106:11 113:5 114:3 206:23 207:6,9 requires 207:13 227:19 230:19 requiring 80:23 research 14:19,20 15:20 16:1 45:4,7 researcher 276:4,13 residual 21:4 resolved 94:7 respect 18:11 96:14 139:10
---	---	--	--

<p>143:19 191:25 254:1 306:22 respective 313:14 respond 10:17 101:25 119:20 responding 223:7 response 90:15,19 141:25 219:17 271:10,16 272:7 275:9,13,16 279:9 298:20 responses 226:8 responsibilities 82:20 84:10 responsibility 32:20 84:13 106:18 107:6 108:12 responsible 17:21,25 18:9 32:15 65:17 108:25 262:20 responsive 64:23 restate 66:15 233:3 275:20 300:23 restroom 262:1,6 result 69:22 263:1 results 79:8 207:14,24 208:1,3,15,17,18,21,22 209:2,3,4 210:7,17 retained 11:13,16 49:6 50:10 retention 50:2 59:16 reverse 132:25 218:4 review 7:9,18,21 29:16 34:4 48:8 62:9,13 100:25,25 161:13 172:2,18 173:14,20 184:9 185:18 199:6 202:10 206:14 207:17,20,22 211:17 236:1,21 237:3,18 237:24 239:6,14 242:2,13 243:19 263:10,12,23 264:4 281:17,20 310:13 reviewed 29:5,12 40:20 43:15 44:8 46:24 61:1 62:19 92:21 123:21 124:21 125:2,4 130:10 145:12,25 163:20 168:14 174:8 183:2 198:18,25 203:10 204:6 234:21 236:19 286:10,22 299:10 reviewing 29:22 44:6 63:15 173:3 174:23 213:18 246:5 263:4 reviews 33:10,12,13 171:4 171:17 172:3,8,15,24 173:23 175:12 203:5,9,20 204:20 206:16 209:23 212:13 239:24 240:8 244:25 245:12,18 307:13 revise 47:23 revisions 44:7</p>	<p>revolves 59:11 revolving 121:4 rich 144:13 richer 144:3 Rickey 147:14 148:18 right 10:8 11:13,22 12:2,16 13:10,18 14:5 16:9 20:24 21:17 22:7,23 25:3 27:19 29:21 31:19 33:6 35:21 36:10 38:17 39:6 41:22 42:14,21 43:4,9 44:16 46:19 48:13 49:24 50:20 50:25 51:8,9 55:14 56:14 57:3 58:19 60:10,17 62:1,2 67:16 70:13 71:3,25 72:3,8 72:14,19,24 73:3,11 74:6 75:17,22 77:6,18,19 78:8 78:11 79:17 80:21 81:22 82:19 83:7,17,18 84:10,16 85:1,2,7,15,16,18,19 86:2 86:7,23 88:3 89:3,10 90:1 90:5,16,21 91:25 93:19 94:23 95:3,8 96:14,20,24 98:10,15 100:8 101:13,19 101:25 102:7,16 104:3,7 104:19 105:3,6 107:17 109:16 111:7,9 113:10,14 113:16,23 114:6 115:20 116:9,19,21 117:3,21,25 118:24 119:4,21 120:1 121:5 122:11 123:14 125:22 127:21 128:7 129:6 129:13,17,19,20 131:3,9 132:1,7,11 133:1 134:22 138:7,8,13,24 139:6 141:12 143:20 145:4,23 147:4 148:7 154:5 156:11 157:2 159:4,8 160:6,20 164:10 166:2 168:12 169:1 169:5,12 170:19 171:18,20 172:8,23 173:3 174:13,17 174:18 175:16 176:8,15 178:21,23 179:4 182:2,11 182:16 183:20,23 184:11 185:14,25 186:8,9,19 188:12 189:4 191:1 192:1 193:3,17 194:14 196:9 197:4,13 200:3,19 201:13 201:19 204:9 205:1 209:20 212:18 213:7,25 214:3,6 214:14 215:4,10,12 217:21 221:18 223:19 224:14 225:16,17,23 226:4 227:2 228:1,6,10,19 230:21 231:7,12 233:12,16,17</p>	<p>239:7,15 240:25 244:4 246:8,19 250:3,18 251:3 251:14 253:25 255:14 258:1,4 259:12,20,24,25 262:8,13,19 263:14 264:7 264:8,10 265:8 266:7,21 267:24 268:9 269:14 270:19,23 271:3,7,13,23 273:16,21 274:2,10,20,22 275:8,11,25 276:25 277:6 278:12,21 282:22 284:9,12 285:3,8 289:15 292:6,21 295:22 296:16 300:11,24 302:1 303:1,6,9 304:6 305:14,20 307:4 308:2 311:16,18,20 Right- 270:2 rights 134:3,25 173:15 risk 34:25 81:24 96:5,10 99:15 105:18,25 106:2 107:14,23 196:21,22 224:16 235:19 247:22,24 248:2,3,6,9,14 269:9,13 277:21 281:17,20,24 282:13 283:4,6,9,15 284:2 284:3,15,17 285:15 286:10 286:21 287:2 289:5,22 risks 34:18 35:13,13 37:5 39:14 113:7 114:5 236:8 283:8,22 284:4,16,25 risky 283:12 risumi 83:25 RMM 236:4 robust 135:16 212:20 300:6 Rohan 89:25 93:2,7 role 29:8 41:12 63:18,24 64:2 68:10 83:23 84:5 86:9 86:10,21,22 88:15,21,23 97:4 111:16 112:4 132:24 134:18 136:13 153:1 293:20 role-based 122:12,22 123:12 124:14 126:4,22 127:12 132:24 135:9 137:4 137:23 140:24,25 141:3,7 141:22 142:12 148:25 150:8 157:11 158:10 162:23 165:24 166:13,16 167:25 168:11,16,25 169:23 170:4,14 173:22 174:24 175:9 179:2,23 181:22 role/access 132:4 roles 86:9,17,18 97:8,10 132:22 133:2,3,10</p>	<p>rooms 79:2 rose 100:16 101:10 rough 311:24 routine 262:23 routinely 261:25 262:6,12 row 285:22 286:2,7,25 ROZALIA 4:21 ROZI 4:21 Rule 46:4 rule-based 288:7 rules 10:10 103:8,19 185:8 run 16:15 running 71:9 Russian 280:3</p> <hr/> <p style="text-align: center;">S</p> <p>S 3:1 4:1,12,12,17,17 S-A-R-F 123:22 S-O-C 41:15 S-O-X 40:5 safety 227:1 302:14 salary 82:8 sample 130:16 171:24 204:6 205:11 samples 123:21 124:8,10,20 125:21 126:13 128:19,21 130:23 131:13 138:25 139:11 145:12,22,25 146:19,24 155:3 159:12,16 163:25 168:3 171:17 204:10,24 209:17 211:12 sampling 126:7 SANS 22:15 Sarbanes-Oxley 71:19 SARF 6:17 125:17 126:25 127:1 128:22 129:12 130:7 131:17 134:15 135:2 139:23 142:1,6 145:12,15 145:25 150:2,5 152:13 155:11,24 156:18 160:14 160:16 161:9,12 162:13 168:10 169:15 174:21 178:17,20,21 179:12,19 180:16,17,18,24 181:4,13 181:19 SARFs 123:22,23 124:12 125:6 126:15 127:24 129:23 131:13 139:1,6,7 139:12,16,19 141:2,9,12 141:16,21 142:10,19 143:6 143:10,17,23 144:9,17 146:22 147:4 155:4 157:14 159:13,24 160:2,4 161:5 161:21 162:7 163:2,9,21 163:24 164:6,8 168:14,22</p>
--	---	---	---

<p>169:6,15 173:13 177:19 181:20 204:15 save 314:8 saw 80:8 92:6,9 154:1 155:19 188:10 212:15,16 234:19 saying 10:14 27:12,15,16 54:16 56:1 59:11 73:18 76:21 123:10 142:5,9 144:20 156:17 161:22 178:6 208:14 226:1 252:8 266:19 291:14 295:17 says 77:15 78:13,14 81:23 82:4,19 83:8,15 84:1,8 85:15,24 92:15 93:1,9,20 93:21 94:6 95:16 100:12 114:17 115:9,18 117:12 119:16,17 121:7 122:20 135:6 140:4,23,25 143:3 160:3,12,13 165:8 166:9 167:18 173:12 186:23 188:21 193:20 195:13 218:8 220:22 221:16 225:21,24 233:10 237:3 241:13 258:5,7 289:1 scans 210:18 scheduling 207:13 school 13:25 14:3,6,7,9 45:16 science 13:6,7,8,9,10,16 14:13,15 82:2 scope 57:9 98:7 103:5,9,11 144:24 157:7 158:22 scoring 111:22 screenshot 183:20 184:23 215:7,9 305:17,24 scrub 199:17 SDL 33:17,18 34:6,8 200:12 206:7 214:3 293:11,17,24 295:6,12,15,16 296:10 304:10 309:19,23 se 108:4 Sean 4:5 218:8 Sean.berkowitz@lw.com 4:10 search 64:8,13 SEC 9:14 10:6 50:8 51:15 52:11 53:23 315:3 SEC's 50:3 51:6 52:5 second 39:8 40:3 71:2 83:15 84:7 86:24 92:15 93:21 100:11 109:21 115:22 116:8,16,25 127:9,22 176:10 179:5 208:5,9 225:1 238:15 284:13</p>	<p>288:24 291:6 292:24 301:4 302:1 second-to-last 140:20 188:16 217:23 secret 68:5,22 90:24 91:2 93:21 secrets 68:20 section 123:19 197:19 243:6 sections 210:13,20 236:19 238:16 sector 99:15 100:14 secure 32:24 33:3,5,11,14 203:23 212:11 214:25 250:15 292:11 293:1,11,21 293:22 294:4,18,23 295:9 295:19 303:20 304:15,22 305:1,7,10 secured 304:4 securities 1:4 3:4 24:10,25 53:22 70:3 73:15 74:8,12 75:2,6,11,16 96:22 102:10 120:12,23 122:21 123:11 128:25 135:8 136:22 140:3 140:17 142:3 143:19 144:25 145:2 153:14 157:12 158:24 166:16 167:24 168:24 170:9,10 173:17 179:24 180:21 181:24 188:14 189:19,24 190:3 191:5,21 192:24 193:24 194:14,24 196:7 197:9 206:7,12,21 212:8 229:24 234:9 240:2 244:19 246:14 250:17 255:7 256:22 258:18 290:22 291:11,15 310:22 security 6:11,15 7:9,15,18 7:21 12:22 13:1,21 14:3,17 14:22,24 15:6,10,14,16,18 15:22 16:19 21:23 22:22 23:1,2,8,12,19,23 24:3,4 24:14,20 25:6,12,16 26:1,4 26:6,8,19,21,24 27:4,5,12 27:14 28:14,17 29:4,10 30:14 32:7,15,21 33:7,12 34:12,16 35:13,15 37:1 39:12 40:24 52:12,15,16 64:21 68:11 69:1 73:8 74:19,24 75:13,21 76:4 83:9,16 84:5 85:11,24 86:9 86:18 89:16 92:13,18,20 93:8 94:17 96:16,25 97:3,7 97:13,22 98:1 119:7,17,18 119:20 120:2 121:15,18,20 121:23 125:11 129:18</p>	<p>130:1 139:25 142:7 144:1 151:5,7,10 152:18 153:9 153:12,16,17,23 154:3 156:9 158:10,14 159:1 167:13 175:6 187:13,24 188:6,7,11 194:7 196:21 196:24 198:4,25 199:2 201:2 202:17,22 203:5,9 203:17,20 204:20 207:1,9 207:12,15,17,19 209:22 210:15,16,21 211:17 212:10,13,24 214:8,23 218:11,13,24 219:6,18,20 219:24 220:6,10,14 221:10 221:15,17 222:14 224:6,16 224:19 225:9 226:2,13,24 227:5,22 229:2,6,6,22 230:17,19 235:19 236:20 236:22 238:8,13,18,19,19 239:24 241:3,14 242:7,22 243:19 244:6 245:2 246:2 246:3 249:2 254:25 255:5 255:11 256:2,8,10 257:4,8 257:9,16 258:3 263:19,20 271:14 272:6,16,21,24 273:3 274:17 275:1 276:3 276:12 277:25 278:10 281:10,12,14,16 284:4 288:16,17,22,22 290:14,21 290:21 291:24 292:1,16,20 292:23 294:7,12 295:5,8 304:7,19 307:13,19 310:12 security-related 98:20 236:23 see 10:16 24:4 26:9 36:23 36:25 38:16,25 44:7 64:4 77:21,22 95:16 96:24 100:20,21 109:23 112:19 112:23 113:16,16,18 117:9 117:14 118:8 119:21 120:20,21 123:2,9 130:25 131:24 132:25 133:4 134:25 137:9 140:21 142:6 144:25 145:6,9,16 148:3 148:11 149:23 151:15,22 155:14 157:1 159:18 161:13 164:2 170:12 171:5 173:6 179:9,23 181:2 183:5,16,25 187:14,25 188:20 189:1 191:11 193:8 197:22 199:4,18 201:8 204:8 206:16 208:2 213:24 217:22 220:19,25 222:8,16 228:25 229:4 231:12 232:18 233:13 234:6 235:6</p>	<p>235:16 236:25 237:7 241:5 241:15 244:8 245:3 247:1 249:9 250:23 251:1,1 286:2,4,6,10,12,15,23 291:23 300:19 301:21 seeing 127:15 166:24 297:15 seek 269:2 293:6 seeking 27:7 186:24 229:11 seen 23:24 24:5 41:18 42:7 92:3,23 119:10 129:23 130:14 152:14 174:3 176:16 177:11,24 178:3 179:11 181:4 210:25 219:22 232:20 235:6 236:17 249:23,25 250:4 253:2 284:5 301:16 308:18 308:25 sees 114:20 seize 93:22 select 63:19,21 selected 124:9 145:23 146:20 149:12 204:10,21 204:21,23 205:4 211:12 239:18 selecting 63:18 selection 124:17 self-assessed 110:4 self-assessment 110:24 self-evaluation 111:11 selling 197:10 semantic 85:20 send 43:18 sends 183:19 senior 82:22 84:14 sense 15:24 80:4 125:12,24 157:7 192:5 232:17 233:23 296:6 sensitive 143:3 167:19 sent 92:21 sentence 53:21 54:8 69:25 73:22 78:14 84:8 85:9,10 86:24 93:9 94:16 114:1,11 114:13,25 115:3,15,17,23 115:24 116:5,8,8,16,18 117:1,2 123:2 140:24 143:2,2 155:2 158:7 159:11 165:3,8 167:16 176:10 177:15 179:6 188:3 188:21 189:6,15 191:18 192:2,3,14 193:20 194:16 195:13 210:12 213:17 215:13 220:22 237:18 238:15 239:20 240:13 241:2 242:14 243:25</p>
--	--	---	---

244:21 245:6 251:2,17,20 252:7,14 253:25 265:2 287:17 288:24 291:25 298:2 301:4 sentences 167:10 195:16 199:12 251:22 sentiment 218:12 separate 20:25 28:11 48:2 65:25 180:24 288:13 289:2 292:16 separately 8:8 211:4 separating 289:7 separation 290:24 292:5 sequential 162:1 series 206:24 259:23 260:11 278:2 299:13 serious 258:22 259:6,24 263:14,22 281:8 Serrin 3:17 11:20 49:8 Serrin.turner@lw.com 3:22 served 48:12 Service 90:24 91:2 93:21 services 11:14 99:14 106:17 serving 48:24 sessions 61:10,12 set 20:3 28:20,23 36:16 37:23 47:11 55:5 66:12 81:15 117:5 121:7 125:8 141:19 143:4 144:3,13 155:17,21 167:20 169:8 172:7 173:1 174:9,12 181:21 185:21 200:17 202:19 206:20 211:9,15 212:12 214:18 235:18 255:6 269:11 275:6 281:13 285:21 288:2 290:21 304:24 313:15 sets 71:23 125:1 209:19 setting 31:23 32:1 52:19 settings 305:18 severity 277:17 281:3 share 94:8 shared 218:9 221:17 225:9 shareholders 104:1 sharing 219:11,14,22 220:4 220:12 221:3,11 226:10 227:3,13 Sheet 5:14 314:10 315:1 shift 122:11 short 54:25 65:4 185:11 229:14 shorter 42:3 Shorthand 2:11,14 show 40:23 123:18 128:8 143:7 169:15,16 174:20	180:11 181:12 187:2 208:1 210:19 224:1 236:6 242:18 246:10 283:7 284:16 285:4 300:11 310:20 showed 104:2 125:22 150:14 173:25 185:23 showing 69:4 71:14 130:9 186:20 223:9 239:10 306:19 shows 178:22 205:15 207:13,20,20,23 277:23 281:9 287:1 306:9,12 307:17 310:23,24 side 32:1 48:3,3 77:25 78:1 signature 278:24 279:10,13 279:23 313:17 signed 280:10 314:16 315:24 significant 71:12 203:10,13 203:18 222:14 224:6,8,19 226:2,13 227:5 230:17 261:4,8,12,14 264:4 279:11 similar 24:7 31:1,13 41:16 77:21 78:10 80:13 96:4 100:3 113:21 114:8 125:7 146:18,21 200:15 204:12 205:1 209:19 245:13,20 273:4 simple 19:20 20:8 56:22 240:11 244:5 simply 75:8 242:4 251:24 253:5 simulate 300:16 301:7 Simultaneous 102:20 123:5 163:17 231:20 267:5 270:4 290:15 307:22 308:13 single 173:8 211:24 215:20 245:25 261:20 singular 76:14 108:17,24 260:2 261:17 278:3 sir 10:7 18:24 53:10 62:2 69:24 94:13 96:17 100:8 104:7 109:20 112:16 119:15 122:12,24 123:17 145:4 154:5,19 155:2 166:2 170:19 172:11 175:16 182:2 187:5 197:13 200:10 213:1 230:25 250:18 264:11 285:18 311:17 sit 52:6 275:24 situation 24:7 38:10,23 68:2 68:3 94:7 106:9 151:17 170:1 217:6 219:13 223:9	266:3 267:14 273:4 275:4 276:9 280:11,18 282:8 284:22 288:1 299:7,8 306:18 situations 70:19,19 272:5,9 272:19 284:4 skill 20:3 skills 19:16 20:19,21 29:25 31:14 SkyWest 113:14,16,21 120:1 slide 7:8 199:15 200:11 202:10,15 306:22 309:19 309:23 310:3,5,15 slightly 100:16 small 38:16 82:12 90:11 93:17 255:25 256:6 296:4 SOC 41:17,18,20 71:19 software 15:6,14,15 21:3 32:11,16,22,24 33:15 35:4 197:20,25 198:5,11 203:11 203:16 206:11 235:20 236:3,8 238:19,20 249:3,4 280:5,9 292:12 293:1,22 294:4,19,23 295:9,19 296:1,4 299:13,22,25 300:4,14 301:6 304:20 305:1 Solar 64:25 SolarWinds 1:7 6:15 7:7 9:14 11:24 12:7,8 24:4,7 24:17 25:3 45:24 50:4,8 51:6 52:5,14 59:17,18,21 59:24 64:22 65:1,3,4,7 67:13 70:1 71:12 73:20 75:15 76:20 97:19 119:17 120:14 126:15 129:15,25 132:21 133:9 140:4 149:25 150:7 151:8,22 152:8,13 153:9,11,17 157:10,20 158:25 165:9,17,23 168:4 170:12 174:8 182:24 186:24 187:10,22 190:5 194:10 196:16 197:3,9,10 197:12 198:22 200:12 202:16 206:6 215:19 218:10,24 219:17 229:2 234:12 246:4,6 252:23 254:23 255:19 256:23 258:8,14 263:18 276:4 277:24 280:5 281:10 287:1 288:13 289:1 290:1,11,20 291:5,16 299:10,17 300:9 302:20 304:4 306:25 307:18 315:3	SolarWinds's 22:22,25 23:17 53:25 54:17 119:7 121:15,22 128:23 145:1 158:9 166:12 191:6,8 194:8 197:1 203:11 206:11 220:6 221:10 234:8 240:7 250:16 252:18 258:5 265:5 265:12 305:22 307:7 sole 158:8 214:24 solely 150:14 252:20 soon 260:10 sophisticated 20:10 280:3 sorry 53:14,15 78:5 89:13 106:3 110:14 122:14 145:7 146:8 158:3 166:21 170:22 190:22 211:23 221:20 238:10 262:5 sort 14:19 26:5 29:25 30:16 30:24 31:14,25 33:13 34:9 35:12 36:22 37:20 38:3 39:3,16 40:14 43:7 51:16 51:17 66:15,20 71:17,25 73:6 76:2 79:20 96:10 97:20 101:14 105:14 108:21 112:20 117:25 123:18 125:1,8,22,23 126:1,3 127:18 130:14 133:11 136:21 139:20 148:15,23 150:25 152:7,18 153:1,19 155:23 158:13 169:25 178:5,13 179:25 187:8 196:22 207:17 211:24 212:6,8 215:18,22 219:21 228:25 229:17 230:7,23 232:11 234:11 235:16 241:1 243:20 244:11 247:10,15 248:5 251:10 256:18,23 257:6 258:3 260:2 263:6 265:16 269:4,11 271:9,20 274:24 280:11 281:7 283:10 284:20 285:19 288:6,7 292:16 294:2,8,25 295:18 301:24 308:7,25 sorting 221:20 sorts 65:19 98:18,19 154:2 169:11 207:14,24 267:11 306:2 sotto 188:15 231:5 264:14 source 166:10 186:14 294:25 sources 66:13 157:8 158:12 173:24 204:3 229:21 253:13 294:18 SOUTHERN 1:2
---	---	---	---

SOX 40:5,9,19,23 41:2,10 222:15 224:6 225:2,7,10 226:2,16,20,24 space 49:23 spans 285:22 speak 61:17 114:12 speaker 102:22 123:7 270:6 307:24 speaking 96:25 103:12,19 184:15,25 185:1,3 188:15 231:5 264:14 spec 234:16 specific 14:8 17:14 20:7 25:8 27:9 36:6,16 51:16 77:5 79:5,13,15 106:14 112:9 115:12 128:13,18,19 128:20 137:10 144:9,22,23 147:17 149:4 151:17 152:8 164:24 177:22 180:13,15 210:9 219:13 220:11 225:7 225:10 226:16 234:22 235:12 236:11 239:21,22 240:14,15 242:15 243:25 244:11 245:10,23,24,25 248:25 249:18 250:1,7,13 254:17 258:16 266:3 268:8 271:19 275:4 276:8 278:19 283:25 284:1,8,22 285:4 287:5,6 302:9 304:24 306:18 specifically 66:6 99:5 100:6 113:25 118:4,18 147:13 208:2 235:11,21 252:6 276:19 284:11 288:23 specifications 113:4 114:2 115:13 specifics 25:15 34:10,11 46:24 47:4,8 55:24 91:21 94:5,10 115:8 165:20 177:19 specified 176:13,17 177:9 178:10 specify 31:8 speculated 234:16 speculating 178:12 180:5 speed 206:3 281:6 spell 22:11 spent 12:14 split 83:3 spreadsheet 285:16,19 287:1 Spring 96:13 sprint 199:17 SRM 7:9 stage 33:12 81:25 245:2	stages 268:24 stakeholders 100:19 101:7 101:13 stamp 205:13 232:8 237:15 285:14 stamped 217:19 stand 94:15 standalone 141:12 standard 39:18,21,25 69:25 70:5,20,23 71:22 75:23 76:3,8,15,19 77:5 114:19 118:11 133:2 156:21 179:7 179:14 180:3 295:12,20,22 295:24 296:8 297:3,5,9 standard-setting 118:14 standardized 133:8 standards 35:22 36:3 75:25 113:1,4 114:2 115:12,19 116:23 117:6 120:15 121:8 standing 141:9 standpoint 80:18 136:3 162:25 start 69:12 184:5 213:10 277:13 started 28:2 308:6 starting 28:1 46:11 223:14 298:17 307:18 310:9 starts 112:17 175:18 181:16 205:12 234:1 269:13 state 2:12 52:15 105:1 108:2 123:21 166:6 167:22 187:9 190:20 194:6,18 198:17 232:11 236:17 313:24 stated 115:5 117:11 118:6 179:24 208:21 236:2 252:24 310:8 statement 6:16 22:23 23:1,8 23:19 24:4,10,17 26:1,8,19 26:22 27:4,6,10,12 52:13 52:17 55:21 57:10 58:5,14 59:4 70:3 72:7,18,23 73:5 73:9,15 74:8,13,19,24 75:3 75:6,11,21 93:6 96:23 97:19 98:1 100:22 102:10 109:8 113:22 116:1 119:7 119:24 120:3,12,14,16,17 120:23 121:16,18,20 122:21 128:25 129:18 130:1 135:8 136:23 139:25 140:4,17 142:3,7 143:8,19 144:2,25 145:2,6 151:5,7 151:10 152:18 153:9,12,14 153:17,23 154:4 156:9 157:12 158:7,10,15,24 159:2 166:16 167:14,25	168:19,25 170:9,11,17 173:17 175:6 178:9 179:25 180:10,21 181:24 187:13 187:22,24 188:6,7,11,14 189:7,19,24 190:3,12 191:21 192:24 193:24 194:14,24 196:8,24 197:10 206:8,13,21 207:12,16 212:10,24 217:6 220:6,10 220:14 221:2,10,15,17 222:18 224:25 229:24 230:24 233:25 234:10 238:5,9,10 240:2,6 244:19 246:2,3,14 250:17 252:20 253:4,19 255:1,8,11 256:2 256:8,10,22,22 257:4,9 258:3,15,18 263:19,20 274:11 281:14,16 288:22 290:22 291:11,15,24 292:16,20,24 304:7 306:9 310:22 statement's 123:11 191:5 194:7 statements 23:2,23 24:2,14 24:20,25 25:11,19 26:4,24 27:13 52:23 96:25 97:3,7 97:15 98:14,19,22 99:3,4,8 99:9 100:24 102:9 115:6 144:16 206:12 212:8 307:10 states 1:1 2:18 112:24 118:10 193:5 255:5 278:22 287:15 static 212:25 statistical 156:1,24 158:16 statistically 155:17,21 steal 154:13 stealthily 271:15 stemming 283:8 Stenographer 1:22 47:19 102:22 110:12 123:7 161:10 165:5 219:8 256:14 270:6,8,11 307:24 311:23 312:1 stenographic 9:16 step 245:18 steps 39:17,18 100:17 101:4 214:8 245:17 246:15 248:16 Steve 294:11 stipulated 119:8 stock 100:14,15 101:10,12 stockholders 101:13,18,20 101:23 102:3,9,13 stolen 262:10	STONE 3:9 stop 176:15 218:11,14 222:11 225:22,25 254:3 stopped 58:3,11 59:8 96:19 stories 210:14 straightforward 19:23 strategy 17:6 81:24 82:24 96:4,9 stray 213:22 215:14 Street 3:10 strong 30:5 56:18,24 128:15 144:17 179:1,21 180:18 206:17,19 212:14 216:6,7 216:7,11 240:18 246:23 261:18 274:10 281:10,15 306:7 structure 38:7 89:8 206:25 226:25 260:5 269:7 298:14 298:22 302:9,12,13 structured 78:17 298:5,9 299:2 302:5 structures 18:6 26:13,25 34:25 36:6 41:21 112:9 study 14:11 studying 186:18 subject 74:17,22 94:25 103:3 148:1 submitted 180:25 subparagraph 300:25 subset 169:9 205:4 substance 46:3 239:14 251:4 substantive 138:19 substitute 274:9 substitutes 274:17 suffer 100:14 suffered 90:4 sufficient 126:2 144:20 180:20 181:22 suggestions 46:22 Suite 4:7 summaries 210:7,17 summarized 209:5 summary 209:3 summer 105:9 Sunburst 51:21 279:17 280:2 supplier 196:15,16 support 97:16 99:17 240:6 253:3 supported 106:15,16 supporting 203:25 211:18 supposed 121:8 134:4 261:25 sure 12:5 14:25 22:16 23:7
---	---	---	---

<p>23:13,15,15 24:22 50:16 54:9 56:8 58:8 66:16,17 72:16 74:21 75:12 95:2 110:19 113:15 118:12 122:9 123:1,3 126:8 128:14 129:3,10,10 136:6 139:17 146:13,15 147:25 147:25 156:15,15 161:20 164:5 165:2 167:4 168:21 171:7 173:2,8 176:2,21 180:19 182:7,7 183:8 189:18 190:12 191:13 199:7,8 200:5 205:18 210:25 224:14 233:2,4 243:12 247:7 253:9 256:4 259:4 264:2 269:24 276:21 276:24 277:3 282:11,13,21 286:14 293:18 297:24 302:23 304:19 310:17 surprise 296:13 SW-SEC-00166790 232:9 SW-SEC-00254254 217:19 SW-SEC-00296522 171:24 SW-SEC-SDNY- 131:20 SW-SEC-SDNY_00050922 177:3 SW-SEC-SDNY_00055006 241:11 SW-SEC-SDNY_00055119 205:13 SW-SEC-SDNY_00069825 237:16 SW-SEC-SDNY_00184276 200:2 SW-SEC-SONY 7:10 SW-SEC-SONY_00047323 6:22 SW-SEC-SONY_00049602 6:20 SW-SEC-SONY_00050922 7:6 SW-SEC-SONY_00055006 7:23 SW-SEC-SONY_0005545 6:18 SW-SEC-SONY_00069825 7:20 SW-SEC00166790 7:17 SW-SEC00168780 8:6 285:14 SW-SEC00254254 7:14 swear 9:19 switch 182:2 265:4 sworn 5:11 9:21 313:3 synonymous 168:17 169:24</p>	<p>247:24 system 20:22 31:10 89:7 133:4 140:12,13 143:11 169:8,16 173:2,7,19 175:8 175:9,10 179:3 273:3 282:5,7 systemic 255:22 262:3 265:15,17,25 266:2,24 269:6 systems 1:24 16:10,14 17:2 21:23 30:8,10,11 31:20 41:5 76:11 136:12 141:1,5 143:4 165:20 167:19 193:7 193:14 195:14,21 257:25</p> <hr/> <p style="text-align: center;">T</p> <p>T 4:12,17 table 238:3,4 240:5 241:15 241:18 242:21 tactics 28:20 29:18 take 10:21 11:1 16:21 34:18 39:13 40:22 50:15,16,17 83:23 88:20,22 94:25 100:17 101:5 131:9 164:17 172:19 183:10 191:12 200:4 217:4 227:9,23 236:12 258:10 262:2 270:21 300:20 302:21 305:3 taken 2:4 10:7 13:12,14,15 15:13,15,17 16:6 26:18 50:23 81:18 95:6 138:11 143:25 182:14 228:4 271:1 303:4 313:5 315:2 takes 231:4 254:2 talk 10:15 91:20 110:3 138:21 224:20,22 230:23 243:14 259:13 268:8,14,15 299:2 talked 39:9 49:3 68:25 96:15 96:25 130:21,22 165:22 173:12 178:4 204:5 207:7 244:3 252:20 302:11 305:16 talking 18:21,21 20:21,25 23:8,16 38:1 55:25 72:11 97:3 112:8 142:17 145:18 149:5 150:20 169:25 175:22 176:20 197:8,20 201:10 204:14 214:5 219:12 221:7 225:20 228:17 230:14 243:25 252:10,12 253:4,5,22,24 262:15,16 263:17 266:18 269:25 270:13 272:4</p>	<p>278:12 283:25 284:7 285:5 287:5 289:9,11 290:13 292:8,15 302:2,12 309:25 310:1 talks 86:24 87:20 145:10 194:19 207:11 251:17,18 277:16 292:4 task 96:22 180:12 188:5 266:5 268:17 team 6:11 12:4 16:15 17:10 17:15 61:4,6 78:16 79:3,24 79:25 80:7,15,24 81:5,16 82:22 84:13 92:13 93:17 96:9 100:4 106:22 107:1,1 107:5 111:21 134:21 135:12 138:21 195:1 197:6 197:11 204:17 244:6 245:1 245:12,19 249:15,21 275:9 298:4,20 302:4 teaming 298:13,25 teams 21:5 34:5 65:16 78:14 79:1 170:11 196:14,14,25 197:7 207:2 236:7,24 238:6,17 242:9 249:25 252:9,12 253:6 294:6 298:3 technical 17:22 18:1,6,12,13 18:15,21,23,25 19:15 20:15 29:25 31:14,18,21 80:18,25 81:10 113:4 114:2,19 115:12 120:15 121:8 136:3 162:25 191:9 192:12 194:11,22 techniques 28:20 29:18 technologies 115:20 216:10 technologist 19:21 technologists 202:8 technology 13:14 14:11 15:20,21,22 34:5,17 35:23 37:2 113:1 134:8,21 192:17 202:20 229:3 288:2 288:4 Technology's 116:23 tell 46:2 49:23 70:24 131:12 134:2 141:3,9 149:13 150:12 160:22 164:15 171:21 172:17 205:15 206:4 274:5 300:12 telling 253:1 tells 116:4 136:12 temp 179:8,14 180:4 temp's 181:5 template 206:24 templates 238:16 242:6 temps 176:14,18 177:10</p>	<p>178:2,11 tend 227:18 284:21 305:1 tends 302:16 tenets 220:5 tens 267:8 term 54:8,14 56:24 219:10 234:4 247:4,6,8,11 248:14 279:16 293:12,14 296:17 303:20 304:17,21 termination 181:1 terminology 51:16 248:5 terms 16:14 30:10 31:22 34:23 40:17 41:19 46:11 56:10 61:23 64:8,13 70:14 71:5 81:9 93:15 97:2 115:12 125:12 134:16 144:15 147:12 148:25 156:9 158:16 172:21 174:1 174:14,19 175:7 177:24 190:11 192:10 200:22 209:3 212:22 226:20 229:1 238:17 243:9 247:14 248:24 252:18,25 258:2,14 269:16 283:15 293:5 298:15,22 301:18 303:19 306:17 308:23 test 81:17 207:14 208:1,3,15 208:17,18,21 209:4 216:18 tested 301:22 tester 301:17 testers 311:9 testified 9:23 138:1 186:11 300:9 testify 11:10 69:19 103:1 testimony 43:15 47:18 48:17 71:13 103:6 135:11 141:13 143:22 150:16 184:19 186:23 194:2 251:9 251:25 252:2 306:17 313:7 314:5,8 testing 17:11,15 78:15,17 78:21 79:6,15 198:25 199:2 201:2 204:4 207:11 207:13,14,23 209:14,16,23 210:10,16 212:12,25,25 296:17 297:2,8,12,16,18 298:4,6,10,12,17,21,25 299:2,4,11,15,19,21,22 300:3,6,14 301:5,5,11,19 302:5,6,16,17,18 311:4 tests 79:3 81:19 210:18 Texas 2:10 text 188:17 thank 18:23 29:21 53:18 123:16 162:3 187:8 205:21</p>
---	--	--	--

219:4 227:10 287:8 303:11 303:12 311:17 thanks 50:18 132:12 138:7 270:21 theoretically 152:11 268:16 272:18 276:1 thing 10:24 11:3 27:15,17 48:8 172:20 264:7 things 19:3 26:15 28:23 30:5,8 32:1 38:22 53:9 57:11 65:19 74:4 75:15 77:23 81:15 86:16 97:14 98:18 99:14 116:4 117:25 136:17,25 140:11 142:19 144:21 148:23 152:19 158:14 178:25 183:8 186:20 188:7 192:5 196:17 196:18 204:4,18 206:3,22 206:25 207:7,10 210:1 212:3,23 214:19 217:22 227:18 229:5 238:21 240:13 242:11,19 244:7 246:24 248:12 255:7 257:6 257:13 265:21 267:12 281:16 304:18 308:5 310:8 think 20:6,13 24:3,20 27:8 27:16 29:15 30:23 35:18 36:15 37:8 38:14 39:20 47:14 55:5,6 56:11,25 60:5 60:9,12 62:5 66:22 74:6 80:3 85:19 86:11,19 88:14 93:14 100:4 103:7 104:11 110:23 115:3,22 117:22 124:24 126:21 129:1 134:16 142:9 149:9 150:24 154:14 155:23 156:8 161:1 161:3 162:14,20 163:4 171:21 172:22 176:7 177:13 179:15 181:9 183:13 184:4,13 194:24 196:6 199:5 204:14,24 223:8,20 224:18 227:3 228:23 229:20 230:16 231:22 234:2 247:17 248:21 249:15 251:15,16 251:23 255:20 256:21 258:11,21 259:5,11 260:1 266:17 267:18 270:13,20 271:12 272:11 273:14 276:18,22 277:3 278:8 279:3 282:15 283:24 286:13 289:19 293:3 297:11,17,17,18 300:22 304:2 305:16 309:21,21 thinking 27:12 97:20 121:4	215:25 272:22 third 53:21 100:9 143:2 201:5 208:9 285:23 thorough 127:18 thoroughly 291:25 thought 139:21 214:3 224:16 234:25 thoughtful 180:19 thousand 83:12 86:25 87:3 93:16 94:20 123:22 125:5 thousands 145:12 177:19 179:12 267:8 thread 221:19 threads 218:4 threat 17:14 34:14,23 35:3,5 35:7,10,18 36:6,9,14,21 37:9 39:10,15,19 207:8,8 207:10 231:11 232:14,16 232:21,24 233:10,20,22 234:4,7,9,13,17,19,24 235:1,4,7,11,12,17 236:1,7 236:18 238:12 239:3 240:1 240:21 242:17,19 244:9,12 244:17 246:7,8,12,13,22 247:3,11,13,20,21,23 248:2,6,9,13,17,22 249:9 249:12,16,19,20,24,25 250:4,8,10,14 252:11,19 252:22 253:5,7,14,23 295:4,7,11,20 296:2,7,10 305:8,11 threat-based 34:18 37:4 39:14 threatened 93:22 threatening 248:24 threats 34:21 35:14 37:1 39:14 three 61:10 113:18 114:7,11 236:4 287:19 thresholds 269:11 ticket 6:19,21 7:5 147:10,25 148:17 150:1,3,23 152:13 161:14,15 164:23 175:23 178:16 179:5 181:4 ticketing 165:1 174:22 tickets 139:5,9,12,14,15,18 139:24 142:2,6 143:18 144:9 145:10,13,22 147:5 148:20,22 150:6 155:5,12 155:25 159:14,23 160:3,13 160:15 161:7 162:7,17 163:8,10,16,21,24 164:6,8 164:8,11 168:14,22 169:7 169:16 179:12 210:13,21 211:23 212:16	Tim 46:18,23 52:6,14 183:2 224:16 286:11,16,22 time 9:10 10:21,22 14:21 15:1 50:20,25 53:25 54:18 56:4 62:12 67:21 70:7 82:6 83:3 87:24 88:1 90:19 91:14 92:6 95:3,8 102:23 105:5 118:19 123:8 129:9 131:10 132:9 136:20 138:8 138:13 157:1,23,24 164:17 166:7 176:12,13,17 177:9 178:1,10 182:11,16 183:10 191:2 201:16 211:21 223:22 224:3 228:1,6 254:24 256:3 257:24,24 262:1 263:9 269:10 270:7 270:23 271:3 288:3 303:1 303:6,10,11 307:25 311:20 312:4 313:5 times 25:7 26:3 34:15 39:12 40:21 61:8 87:16 98:16 111:22 118:15 142:14 235:7,15 245:17 250:3 268:25 timing 253:10,18 TIMOTHY 1:8 title 96:11 243:6 titled 198:25 today 9:15,18 11:11 47:13 47:14 52:6 60:23 211:3 212:6 234:3 303:11 Today's 9:10 TODOR 3:6 told 219:25 230:12 tools 19:1,5,8,11,13,16,20 20:2,8,11,14,16 32:2,6 79:5,13,15,20 299:14 300:15 301:7,12,19,19,25 top 145:20 241:15 topics 122:11 182:3 total 12:12 61:22 169:9 244:20 270:3,15 touched 37:12 197:24 tracking 154:9 166:20 trade 68:5,20,21 traded 82:17 train 22:4 trained 149:24 training 81:18,20,21 306:22 307:15 310:9 tranche 124:16 tranches 62:17 124:15,22 204:13 transcribed 313:9 transcript 314:5,7	treated 218:20 trees 43:22 trial 69:19 tried 64:22 131:15 trouble 154:9 true 88:16,17,19 90:22 154:4 166:17 168:1 169:1 189:20,23 251:13 274:8 300:17 305:15 306:11 313:7 314:7 trust 53:6 113:14,20 120:1 truth 253:1 truthful 52:22 251:25 252:2 truthfully 11:5,11 try 54:15 267:17 278:9 trying 36:13 38:14,25 46:16 50:5 52:10 54:13 56:21 57:9 65:15,22 67:12 78:19 79:16 80:22 107:13 116:10 121:1 125:9 129:4,11 135:4,7 136:11 155:14 156:13 162:24 166:19 177:21 178:22 185:2 192:1 195:18 216:1 219:19 221:23 231:15,16 238:23 243:13 245:21 249:6 255:13,14 259:11 266:7 269:22 272:23 280:20 283:20 284:14 290:2 302:8 Tufts 13:22 turn 53:10 100:9 104:11 119:15 123:17 145:5,11 154:6 166:5 175:17 190:14 197:14 201:5 213:1 216:13 231:1 236:14 285:23 286:7 turned 53:14 56:19 211:20 Turner 3:17 5:6 12:6 16:11 17:23 18:14 19:7,18 20:5 29:17 30:2 31:17 32:12 40:10 41:7 42:6,10 43:16 43:20,22 44:21 46:10 47:17 49:13,22 50:13,18 52:7 53:16 55:3,23 56:23 57:24 63:2,4,13,20,23 64:18 70:9 72:9,25 73:21 74:25 76:6 80:2 84:18 90:25 95:2 98:6,25 99:10 102:1,8,18,24 103:10,14 103:16 107:16 108:15 109:25 111:5 116:12 118:21 122:2,7,9 127:3,6 127:25 128:2,4 130:2 132:3,8 133:17 134:5 135:20,23 137:12 143:21 148:7 154:8 157:3 158:5
--	--	---	--

<p>160:1,7,12,25 161:19 163:3,14 164:17,19 165:18 168:7 169:2 180:6 181:7 182:10 183:10 184:12,17 184:22 185:1,6,10 189:10 189:17 193:18,25 194:15 202:13 208:6,10,24 210:23 214:4 215:11 218:15 219:7 219:10 222:21 225:4 226:11 227:10 231:19 239:16 240:9 243:8,23 247:5 248:19 251:12,23 254:9 255:2 258:25 259:9 261:6 262:5,11,14 264:15 266:17,24 267:17 269:20 269:24 270:10,12 271:17 272:10 273:9,17,24 274:12 274:14 275:17 279:19,24 280:16 282:21 283:1 287:4 287:24 288:15 289:16 290:13 291:9,13 292:14 295:14 296:20,23 299:20 302:23 303:15 304:13 308:1,15 309:3,8,13 310:1 311:5,7,19,23,25 312:3 Turner's 44:3 195:11 turning 94:13 two 17:7 28:11 48:2,15,16 61:15,15 65:4 77:23 86:8 102:25 148:12 167:10 195:16 241:19 248:12 251:21 279:9 285:22 290:2 302:22 type 24:17 81:4 164:16 196:25 206:15 207:11 227:19 232:14,16 233:20 233:22 258:21 259:5 305:25 308:22 types 16:20 63:14 64:10,21 174:4,15 190:6 210:1 212:2 263:25 267:25 273:3 300:16 301:7 310:8 typical 137:1 144:11 230:4 249:8 typically 249:22 typographical 43:8</p> <hr/> <p style="text-align: center;">U</p> <hr/> <p>U.S 92:16 260:15 UARs 142:19 uh-huh 42:17 67:11 77:11 87:1 89:18 95:15 99:24 100:10 104:10,16 108:11 112:18 113:12 114:23 115:21 120:13 123:20,24</p>	<p>124:6 131:18,21,23 133:14 135:24 140:18 145:8 146:25 147:7 149:7 154:7 157:19 159:22 164:14,21 166:4,8 167:17 175:21 190:19 192:25 197:16,21 198:21 199:19 201:7,17 213:3 216:15,22 217:16,25 220:15 222:6 223:15 227:11 228:15 231:18 235:24 236:16 238:2 243:16 250:20 255:16 258:20 271:25 274:7 277:5 278:14 279:14 282:17 283:5 285:6,20 286:1,16 287:14 292:10 297:21 298:1 301:1 302:3,7 307:2 UK 165:10 Um 274:13 unable 310:4 unattended 262:6 unauthorized 188:24 unclear 233:15 undergo 298:23 undergone 40:19 underlying 243:7,19 underneath 120:8 241:16 undersigned 313:2 understand 11:8 13:18 14:2 35:14 36:14 46:17 52:2 53:22 54:14 58:8 59:2 63:8 63:17 65:15 67:7 78:20 86:13,20 103:14 108:2 116:7,24,25 120:10 121:1 123:16 129:11 135:4,7 139:5,7 148:17 151:8 156:14 158:18 159:24 160:3,13 162:25 163:15 165:5 174:3 191:14 194:7 212:8 219:19 224:24 229:16,19 230:1 243:13 249:7 251:5 252:9 255:15 260:12 266:8 275:17 276:10 279:18 280:20 283:20 284:15 302:9 understanding 12:20 37:24 52:4,11 54:6 56:9 57:2 97:4 114:10 116:17 121:25 137:7 168:22 191:5 196:10 196:23,25 200:12 201:20 202:11 207:8 248:4 276:14 280:2 288:1,12 314:11 understands 170:14 understood 10:20 76:8 190:6 214:22 217:20 304:8</p>	<p>undertaken 81:20 undertook 25:15 106:16 underway 35:17 37:7 underwent 41:17 unfortunately 43:11 uniformly 156:11 unique 220:24 221:15 unit 93:12 UNITED 1:1 units 126:10,18 university 13:15,23 45:15 unnecessary 156:1 192:7 192:22 243:2 unpatched 273:2 unrelated 73:19 unreportable 102:20 123:5 163:17 231:20 267:5 270:4 290:15 307:22 308:13 untrue 256:2,8 257:4 updated 199:1 urgency 223:9 224:1 228:24 229:11,14 230:23 urgently 223:7 use 17:17 19:10 33:18,21,21 47:7 54:8,14 64:8 79:20 109:11 111:9,11 113:5 114:3,21 118:8 126:6 144:5 152:12 164:12 187:4 188:22,25 190:12 191:7 194:9,20 197:2 220:1,1 221:8 230:5 247:19 260:17 268:18 275:24 288:4,10 296:2 301:12,17 306:6 useful 176:22 187:1 215:24 user 6:23 19:23 20:8 30:17 30:20,21 31:3,7,10,15,20 139:8,23 140:14 141:17 142:1,10 143:15,24,24 144:18 149:21 157:22 171:4,17 172:2,3,7,15,18 172:24 173:13,14,14,19,23 174:22 175:2,4,11 194:19 219:24,25 users 31:5 121:22 174:9 175:14 220:23 221:14 uses 304:4 usually 19:10 21:4 25:1 31:3 124:21 283:24 utilize 76:25 utilized 107:19 150:9 185:25</p> <hr/> <p style="text-align: center;">V</p> <hr/> <p>v 1:6 315:3 vague 128:2 308:20 VALENTI 3:18</p>	<p>valid 273:6 validate 126:3 validated 137:4 138:3 141:20 validating 212:23 value 251:11 varies 83:6 268:6 variety 19:19 33:20 35:9 76:25 154:2,2 207:14,24 various 64:20 106:10 198:18 300:16 301:7 308:10 vendor 170:11 190:1 194:25 196:6,8,11,13 197:2,3,7,11 verb 80:19 version 119:13 285:13 versus 37:20 165:21 242:23 243:6 265:17 268:1 video 1:14 2:3 9:12 videographer 4:19 9:6,9 50:20,25 95:3,8 138:8,13 182:11,16 228:1,6 270:23 271:3 303:1,6 311:20 view 55:1 58:5,6 101:22 229:16 234:17 235:1,3 247:21 278:5 305:21 violate 220:5 283:22 284:17 violation 222:15 224:6,19 225:3,10,12,18 226:2,17 226:20,24 283:8 violations 38:16 Virginia 2:19 virtue 153:14 voce 188:15 231:5 264:14 voluminous 117:11,21,23 118:10,13 voluntarily 111:11 voluntary 109:14,15 111:8 114:19 117:13 118:7,11 vs 9:14 vulnerabilities 78:18 298:6 vulnerability 16:16 210:18 248:4,7 301:5</p> <hr/> <p style="text-align: center;">W</p> <hr/> <p>W 92:19 Waack 1:23 2:5 9:19 313:21 Wabash 4:7 Wait 295:14,14 Waived_X_Not 313:17 walk 10:11 205:14,19 walkthrough 206:1 want 23:7,9,13 29:17 36:24 39:7 46:2,15 50:12,17 53:13 54:11 56:8 58:8 62:2</p>
---	---	--	---

63:7,8,13,17 66:17 67:10 71:25 75:12 77:6 79:18,19 94:25 104:7 109:11 113:15 122:2,23 123:1,3 124:4 129:1 139:3 145:17 146:13 154:12 155:8 164:11 170:3 176:15 183:7 191:3 205:24 210:25 216:23 217:10,22 227:18 228:16 251:4,4 252:6 253:8 258:6,7 263:3 264:15 265:9 267:18,25 269:20 270:10,12 274:4 282:3,11,21 283:3 285:18 286:6,13 292:21 303:10 311:24 wanted 24:1 64:4 65:2 91:19 123:18 126:8 136:4 227:21 229:13 232:15 233:21 wants 223:10 WARDEN 3:8 warfare 13:24 28:3,4 92:17 warrant 263:10,11 Washington 2:12,17 3:11 wasn't 15:23,25 25:2 57:8 75:13 77:4 88:25 108:17 134:22 144:8 149:24 150:21 153:1 179:16,22 180:12 216:8,8 252:19 266:4 279:11 281:8 waterfall 198:6,14 Watkins 2:19 3:16 4:4 11:19 12:3 44:25 45:2 49:10 59:17 60:3 way 24:25 26:16 36:14 38:21 59:8 100:18 101:6 109:16 111:9 119:8 120:12 137:1,8 139:17 145:1 161:4,19,20 170:5 174:1 178:8 180:16,20 181:13 224:4 229:1 240:20 252:3 257:5 284:3 285:21 288:2 291:15 297:9 305:2 308:7 ways 36:19 39:23 59:10 297:7 we'll 10:18,21 33:18 40:2 131:5 227:9 we're 10:14 18:20 20:21 23:7,13 27:16 38:6 51:2 53:6 55:25 56:18 95:10 118:19 138:15 143:7 150:25 152:7 176:20 181:10,10 182:13,18 214:5 221:19,25 227:3 228:8 230:14 243:25 256:19 259:18 262:15,16 263:17	264:18,18 270:13 277:5 278:12 285:4 287:12 289:21 293:19 295:17 303:8 we've 32:3 50:14 71:19 79:4 100:4 124:11 130:22 150:20 156:2 157:4 158:7 165:22 168:13 178:4 183:6 188:4 212:6 234:5 244:3 248:21 252:20 weapons 260:17 website 99:23 117:4,10,19 117:20 118:2,10,19,23 websites 117:24 118:15 Wednesday 1:16 2:21 6:3 7:3 8:3 week 83:6,6 weight 151:3 went 38:11 104:1 123:13 170:22 212:1 224:12 weren't 38:12 59:13 WHEREOF 313:15 White 17:6 wide 19:19 33:19 35:9 97:8 97:9 widely 268:6 willy-nilly 178:24 within-entitled 313:4 witness 5:2,20 6:2 7:2 8:2 9:19,22 11:21 12:8 16:13 17:24 18:15 19:8,19 20:6 30:3 31:19 32:13 40:16 41:8 42:8,12 44:22 47:21 48:25 49:8 52:8 53:19 55:4 55:25 56:25 63:3,22,24 64:20 70:10 72:10 73:1,22 76:7,10 80:3 84:21,23 91:1 98:8 99:2,12 102:2 103:21 107:17 108:16 110:2,16 111:7 123:9 127:5,8 128:1 128:3,6 130:3 132:5,11 133:18 134:6 135:24 137:14 143:23 148:8 154:13,17 157:4 158:6 161:24 163:19 164:18,21 165:7,19 168:10 169:3 171:13 177:4 180:9 181:9 182:5,8 183:13 185:5 189:11,18 193:19 194:3,17 202:14 208:8,11 209:1 214:5 215:12 217:4 218:17 219:11 222:22 225:6 226:12 227:11,25 231:22 239:19 240:10 243:9,24 247:6 248:20 251:15 252:1	255:4 256:15 259:1,10 262:15 264:18 267:3,7 269:22 270:17,22 271:18 271:24 272:11 273:10,22 274:13,16 275:20 279:20 280:1,17 287:9,25 289:21 290:17 291:14 292:15 295:17 296:22,24 303:12 308:21 311:8,18 313:15 314:1 witness's 313:7 witnesses 102:25 won 69:23 wonder 233:24 wondering 39:16 129:22 148:15 151:14 243:17 251:8 word 58:12 121:5 123:3 158:3 172:23 188:2 189:4 189:5,8,15 197:2 224:14 273:14 wording's 192:7 words 54:10 247:16,20 work 18:9 25:13,22 26:7 44:14 46:4 59:20,21 60:2,3 64:4 78:8 89:5 106:12 107:22 129:1 210:6 269:6 275:7 281:18 282:9 289:13 290:7 293:10 311:3 worked 41:21 49:12 60:16 65:18 99:15 working 99:13 111:20 164:3 207:3 249:2,21 293:19 works 22:4 78:20 92:19 294:9 World 259:23 260:10 world's 90:4 worries 78:6 wouldn't 81:2 91:3,3 163:12 185:3 210:5,5 263:9,11 274:16 296:7 301:24 write 42:9 44:19 45:3,6,25 51:23 100:2 120:10 223:16 224:3 252:8 287:2,15,19 288:5 289:9,12,23 writes 222:10 writing 26:2 222:24 223:6 written 24:9 58:14 154:16 181:13 193:11 196:1 249:8 249:22 wrong 109:16 111:9 148:5 196:7 300:12 304:3 wrote 13:22,23 28:19 44:22 103:25 232:12,21 233:19 251:10,19 252:3,15	X Y y'all 163:6 yeah 12:15 18:8 21:2 27:16 33:18,18 36:3 40:6 42:25 43:5,24 44:6 48:16 49:20 50:18 54:9 56:16,25 57:20 59:5 60:11 63:3,7 66:19 68:21 70:21 72:10 73:1 75:18 77:25 78:7 84:17,21 84:21,23 87:15 89:13 95:23 96:2,21 100:5 103:24 104:22 105:21 108:16 110:2 114:7 116:10 116:15 117:9 122:5,8 123:9,13 124:24 127:6 128:3 129:21 133:22 134:6 135:4,8 136:8 139:20 141:23 143:24 145:6,7,17 146:13 148:11 153:16 156:20 164:18 165:7 166:25 167:7 170:3 171:8 171:13 175:25 176:22 177:4 178:13 183:21,25 187:16 190:25 193:19 196:10 197:10 198:3 201:12,15 203:7 206:2 208:8,12,12 209:1,6 213:8 218:20 221:22,23 222:1 226:12 227:15 228:13 238:10,19,19 239:10,19 247:6,17 254:17 260:6 261:13 263:15,23 264:17 265:20 267:3,21 270:17 272:11 273:1,10,11,22 274:3 275:23 276:1 277:5 277:8,15 280:1,17 282:6 282:19 283:24 284:19 286:5,8,17 288:16,21,21 288:25 289:21 290:17 291:14 295:17 299:6,7 300:2 305:4 309:24 311:8 311:14 312:3 year 6:11 15:2 56:20 58:3,21 58:25 83:22 92:13 112:22 years 30:25 67:20 69:7 70:7 70:16 88:10 107:19 135:16 yep 11:8 23:18 62:6 77:13 113:18 119:14 127:5 140:22 171:2 197:18,23 217:12 218:6 222:4,9 233:13 yesterday 61:15 York 1:2,17,17 2:15,16,18
---	--	---	---

2:20,21 3:20,20 9:4,4,13 9:13 313:23,23,24	210:25 211:13 121 216:14,17 122 223:14 123 282:16 126 216:17 1271 2:20 3:19 9:13 13 7:12 53:11,14,15 109:18 217:2,15 221:22 228:11 131 6:18 132 277:3,9 14 7:15 231:24 232:7 233:10 235:23 14-or-so 204:24 14420 1:24 2:15 313:25 145 113:11 147 6:20 15 7:18 62:1 122:3,6,7,17 237:9,13 158 187:6,15 159 6:22 16 7:21 240:22 241:8 160 217:18 17 8:5 285:9,13 171 6:24 176 7:6 18 7:13 176:1 19 54:1 176:1 193821 6:19 199 7:8 1998 15:4	2018 54:1,19 55:18,20 57:18 67:15 199:2 200:14 2019 7:13,17 55:20 58:4 77:17 83:8,17,20 84:2 85:4 85:5,6,15 86:2,7,14 94:16 95:17,20 96:17 276:3 2019.2 7:22 2019.4 7:10,19 2020 285:15 2021 54:2,19 55:19 57:18 67:15 200:14 2023 50:12 82:4 96:5,7 112:22 202365 6:21 2024 6:6,9 42:21 43:3 62:20 67:12 96:13 2025 1:16 2:21 6:3 7:3 8:3 9:3,10 313:16 314:8 315:2 205 7:11 20549 3:11 21 145:19,21 146:4,10,11,12 210 236:15 237:15 238:10 240:11 241:2 244:24 21007264 1:24 2:13 313:25 211 250:19 252:7 254:1 212 231:1,8 232:2,12 233:7 212-906-1330 3:21 217 7:14 22 6:6,8 199:2 23 154:6,19 23-cv-9518-PAE 1:6 231 7:17 237 7:20 24 66:7 166:5,21 240 7:23 25 170:21 250 88:3,9 250212JWAA 1:25 25th 313:16 26 46:4 260058 7:5 265 218:1 276 201:8 28 124:7 126:14 131:14 139:1 147:5 2800 4:7 285 8:6	30XI008238700 1:23 2:10 313:24 31 104:12,21,21,25 312-777-7016 4:9 313 5:12 314 5:13 315 5:14 33 190:18,24 330 4:7 337108 140:19 188:17 220:18 346 237:6,14 347 241:4,9 35 182:21 358 232:4 36 109:19 145:21 146:19,24 147:6
Z Zames 91:6,7,8,9,17 93:25 Zoom 65:23 110:11,13 Zouhair 131:24 136:3 137:9			
0 00055119 7:11			
1 1 6:5 41:23 42:4,16,18 44:5 44:12,20 47:12 53:11,17 53:18 66:13,14,23,23 77:9 78:3 104:14 120:7 122:14 145:7 146:6 154:10,17 166:22,23 170:21 182:21 190:15 213:2 223:14 231:1 241:3 257:24 264:13 267:22 277:4 1,000 87:8 1,100 60:8 1:49 138:12,14 10 5:5 7:5 50:19 62:1,1 87:14,16 104:22 124:25 176:23 177:1 267:11,16 10-K 112:21 113:22 114:8 10-Ks 113:13 114:11 10:32 50:21,24 10:44 51:1 100 3:10 204:7 254:24 267:11,16 10020 3:20 101 213:2,16 104 264:12,19,25 265:1 106 199:13,15 200:1 11 7:7 92:21 199:21,25 11/18/19 286:10 11:40 95:4 11:41 95:7 11:55 95:9 112 112:16 114 236:15 115 250:21 116 231:8 118 175:19 119 6:16 175:18 176:10 177:8 179:6 181:11 11958 1:23 2:12 313:24 12 1:16 2:21 6:3,17 7:3,9 8:3 9:3,10 54:2 62:1 205:6,10 207:25 210:20 314:8 315:2 12:52 138:9,12 120 204:25 205:12 209:18	2 2 6:7 21:22 41:15,17,18,20 42:1,4,5,16 43:13 48:1,5 53:17 55:9 62:3 66:24 71:19 73:4 77:10,20 78:1 83:14 95:14 146:8 297:22 297:25 2.5 58:25 2:52 182:12,15 20 87:18 135:21 145:5 146:12 176:3 314:19 200 60:10 200-ish 12:15 2007 69:12 2014 69:12 83:8,17,20,22 84:2 85:1,4,15,18 86:1,6 86:13 90:3 94:16 96:17 104:19 105:3,8,10 2015 83:23 85:1,5,6,18 87:24 88:16 89:3 90:1 92:2 92:8 96:20 199:15 200:11 214:13 308:2,3,6 310:10 2016 199:1 2017 6:17 136:6 183:24	3 3 6:10 69:24 91:22 92:1 285:24,25 297:22,25 3:04 182:17 30 42:21 43:3 92:2 303 5:6 309 5:7	4 4 6:13 73:4 99:18,22 207:22 286:7,9 4:11 228:2 4:12 228:5 4:28 228:7 40 122:13,18,19 123:2,10,14 41 6:6 42 6:9 44 123:19 159:16,25 160:22 162:8 45 145:5,10 197:15 47323 164:15 48 301:2 49 154:6,19 155:3 158:8 159:11 198:17 4960 148:10 49602 147:20
			5 5 6:15 53:15 119:1,5 140:16 157:24 188:14 220:14 269:12 288:20 5:27 270:24 271:2 5:48 271:4 50 124:21 125:2,4,9,16,19 126:6 128:21 130:17 133:24 205:2,3 244:4 50/50 83:4,5 500 83:12 87:20,21,24 88:10 94:20 51 171:16,24 172:4 52 166:23 167:11,22 203:2 53 170:20,23,24,24 171:14 55459 131:22 56 213:4 57 264:12

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION,)	
)	
Plaintiff,)	
)	
v.)	Civil Action No. 1:23-cv-09518-PAE
)	
SOLARWINDS CORP. and TIMOTHY G.)	
BROWN,)	
)	
Defendants.)	
)	
)	

Notice of Errata – Deposition of Gregory Rattray
(February 12, 2025)

I, the undersigned, do hereby declare that I have read the deposition transcript of Gregory Rattray dated February 12, 2025 and that to the best of my knowledge, said testimony is true and accurate, with the exception of the following changes listed below:

Pages and Line(s)	Change		Reason
	From	To	
14:22	information security, but	Information security field, but	Clarification
17:4-6	I helped with the formulation of the nation cybersecurity strategy	I helped with the formulation of the nation’s cybersecurity strategy	Typographical error
17:9	Designed different programs	I designed different programs	Typographical error
[various] ¹	security statement	Security Statement	Typographical error

¹ 23:1; 23:19; 74:19; 74:24; 75:21; 119:7; 121:18; 121:20; 129:18; 130:1; 139:25; 142:7; 151:5; 151:7; 151:10; 152:18; 153:9; 153:12; 153:17; 153:23; 156:9; 158:10; 175:6; 187:13; 187:24; 188:6; 188:7; 188:11; 194:7; 196:24; 207:12; 212:10; 212:24; 220:6; 220:10; 220:14; 221:10;

Pages and Line(s)	Change		Reason
	From	To	
26:11-12	I've conducted numerous assessments of companies, cybersecurity postures, control structures.	I've conducted numerous assessments of companies' cybersecurity postures and control structures.	Typographical error
28:8	operational	operationally	Typographical error
31:22	mostly a process,	mostly a process of,	Typographical error
32:18	do I do coding, I don't do coding	do I do coding?; I don't do coding	Clarification
34:15	In basically the idea	It's basically the idea	Typographical error
34:20	I've been the -- many person	I've been the main person	Typographical error
35:1	attune	attuned	Typographical error
54:10	I could reframe words	I could reframe the words	Typographical error
59:4	to the company	of the company	Clarification
65:9 66:2	Kline	Cline	Typographical error
68:9	in place at Insulet	were in place at Insulet	Clarification

221:15; 221:17; 246:2; 246:3; 255:11; 256:2; 256:8; 256:10; 257:4; 257:9; 258:3; 263:19; 263:20; 281:14; 281:16; 288:22; 291:24; 292:16; 292:20; 304:7.

Pages and Line(s)	Change		Reason
	From	To	
[various] ²	securities statement	Security Statement	Typographical error
72:10	I assume GAAP	I assume by GAAP	Clarification
74:5	controls or password.	controls or password policies.	Clarification
83:25	risumi	resume	Typographical error
84:13-14	the team that CISO is the senior director.	the team that the CISO is the senior director of.	Clarification
93:16	manage	managed	Typographical error
126:20	exclusion	conclusion	Typographical error
111:24	assessment company leadership	assessment to company leadership	Clarification
113:17-18	the digital real	the Digital Reality	Typographical error
134:11-12	This is a process that there's a lot of instances on,	This is a process that there's a lot of testimony on,	Typographical error
140:13-14	by the system access for forms and the user access request.	by the system access forms and the user access requests.	Typographical error
141:16-18	There are SARFs is one of the mechanisms that are used along with user access requests so -- as	SARFs are one of the mechanisms that are used along with user access requests, so that as	Clarification

² 70:3; 73:15; 74:8; 75:6; 75:11; 102:10; 120:12; 120:23; 122:21; 123:11; 128:25; 135:8; 140:17; 142:3; 143:19; 144:25; 145:2; 153:14; 157:12; 158:24; 166:16; 170:9; 173:17; 180:21; 181:24; 188:14; 189:19; 189:24; 190:3; 191:5; 191:21; 192:24; 193:24; 194:14; 194:24; 206:21; 212:8; 229:24; 240:2; 244:19; 246:14; 250:17; 256:22; 258:18; 290:22; 291:11; 291:15; 310:22.

Pages and Line(s)	Change		Reason
	From	To	
144:19	auditors also looking at these	auditors are also looking at these	Clarification
150:5	But I was looking for	What I was looking for	Typographical error
151:25	documents demonstrate	documents that demonstrate	Clarification
155:11	SARF	SARFs	Typographical error
156:2	as we've assessed quite a bit	as we've discussed quite a bit	Typographical error
161:9	[indiscernable]	later	Typographical error
161:14	-- further attached form	-- attached form	Clarification
163:12	wouldn't appear as attachments	would appear as attachments	Typographical error
169:13	So I looked for these for presence of	So I looked through these for the presence of	Clarification
174:16	cleaning and pretty	clean and pretty	Typographical error
175:7	privileged	privilege	Typographical error
176:1	to read 18, 19	to read 118 and 119	Clarification
176:3	20	120	Clarification
195:24-25	And you can enforce where it's feasible to do so.	And you can only enforce where it's feasible to do so.	Clarification

Pages and Line(s)	Change		Reason
	From	To	
202:19-20	Mr. Colquitt's depositions and other technology leaders about how	Mr. Colquitt's deposition and other technology leaders' testimony about how	Clarification
208:2 209:15	checkmarks	Checkmarx	Typographical error
208:19 209:6 210:1 210:4	checkmark	Checkmarx	Typographical error
211:23	had the JIRA tickets	didn't have the JIRA tickets	Clarification
212:9	illumination	to illuminate	Clarification
214:23	where a security fit into it	where security fit into it	Clarification
218:24-25	using a password as a security incident	using a password was a security incident	Typographical error
232:9	SW-SEC-00166790	SW-SEC00166790	Typographical error
238:11-12	broadly you have threat modeling is about	broadly threat modeling is about	Clarification
244:9	if threat modeling	if they were threat modeling	Clarification
246:22-25	it's a strong process that there's no reason to believe that the things that are called for, you know, when they're present and the FSR, didn't happen.	it's a strong process and there's no reason to believe that the things that are called for, you know, when they're present in the FSR, didn't happen.	Clarification
248:14	me is a	me of a	Clarification

Pages and Line(s)	Change		Reason
	From	To	
257:11	haven't	have	Typographical error
288:16	Yeah, in the network security portion	THE WITNESS: Yeah, in the network security portion	Typographical error
294:5	device	advice	Typographical error

I declare under penalty of perjury that the foregoing is true and correct.

Date: March 20, 2025

Signed:

Gregory Rattray